

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ „ЛЬВІВСЬКА ПОЛІТЕХНІКА”

**УПРАВЛІННЯ КОРИСТУВАЧАМИ І ГРУПАМИ, СПІЛЬНИЙ ДОСТУП  
ДО ОБ'ЄКТІВ ФАЙЛОВОЇ СИСТЕМИ У WINDOWS XP**

**МЕТОДИЧНІ ВКАЗІВКИ**  
до виконання лабораторних робіт  
з дисципліни „Адміністрування та безпека комп'ютерів”  
для студентів спеціальності  
7.080403 „Програмне забезпечення автоматизованих систем”

*Затверджено  
на засіданні кафедри  
програмного забезпечення  
Протокол № 6 від 19.02.2007 р.*

Львів – 2007

**Управління користувачами і групами, спільний доступ до об'єктів файлової системи у Windows XP:** Методичні вказівки до виконання лабораторних робіт з дисципліни „Адміністрування та безпека комп'ютерів” для студентів спеціальності „Програмне забезпечення автоматизованих систем” / Укл.: В.С. Яковина, О.Є. Білас – Львів: Видавництво Національного університету „Львівська політехніка”, 2007. – 41 с.

**Укладачі** Яковина В.С., канд. фіз.-мат. наук, доц.  
Білас О.Є., канд. техн. наук, доц.

**Відповідальний за випуск** Федасюк Д.В., д-р тех. наук, проф.

**Рецензенти** Федорчук Є.Н., канд. тех. наук, доц.  
Демида Б.А., канд. тех. наук, доц.

## **Лабораторна робота № 1.**

### **УПРАВЛІННЯ КОРИСТУВАЧАМИ І ГРУПАМИ В WINDOWS XP.**

**Мета роботи:** Навчитись виконувати адміністративні задачі управління користувачами і групами локального комп'ютера під управлінням ОС Windows XP Professional; створювати і використовувати переміщувані та обов'язкові профілі користувачів.

#### **Теоретичні відомості.**

Створення облікових записів і груп займає важливе місце в забезпеченні безпеки усіх операційних систем і окрема Windows, оскільки, призначаючи їм права доступу і привілеї, адміністратор дістає можливість обмежити користувачів в доступі до конфіденційної інформації комп'ютерної мережі, дозволити або заборонити їм виконання в мережі певної дії, наприклад архівацію даних або завершення роботи комп'ютера.

Для роботи з локальними обліковими записами використовується оснащення "**Local Users and Groups**". Управління доменними обліковими записами ведеться централізовано на контролерах домену, при цьому використовується оснащення "**Active Directory Users and Computers**". Управління локальними обліковими записами на контролерах домену неможливе.

#### **Оснащення Local Users and Groups**

Оснащення **Local Users and Groups** (Локальні користувачі і групи) – це інструмент MMC, за допомогою якого виконується управління локальними обліковими записами користувачів і груп – як на локальному, так і на віддаленому комп'ютері. Запускати оснащення може будь-який користувач. Виконувати адміністрування облікових записів можуть тільки адміністратори і члени групи Power Users (Досвідчені користувачі).

Приклад вікна оснащення **Local Users and Groups** приведений на рис. 1.

#### **Папка Users**

Відразу після установки системи Windows XP папка **Users** (Користувачі) містить три автоматично створені вбудовані облікові записи. Два перші записи були і в системах Windows 2000, третя з'явилася в Windows XP.

- **Administrator** (Адміністратор) – цей обліковий запис використовують при установці і налаштуванні робочої станції або сервера, що є членом домену. Вона не може бути знищена, блокована або видалена з групи Administrators (Адміністратори), її можна тільки перейменувати.

- **Guest (Гість)** – цей обліковий запис застосовується для реєстрації в комп'ютері без використання спеціально створеного облікового запису. Обліковий запис Guest не вимагає введення пароля і за умовчанням є заблокованим. (Зазвичай користувач, обліковий запис якого заблокований, але не видалений, при реєстрації одержує попередження, і входити в систему не може.) Він є членом групи Guests (Гості). Цьому обліковому запису можна надати права доступу до ресурсів системи так само, як і будь-якому іншому.
- **SUPPORT\_388945a0<sup>1</sup>** – компанія Microsoft зарезервувала цей запис за собою для підтримки довідкової служби Help and Support Service; запис є заблокованим.

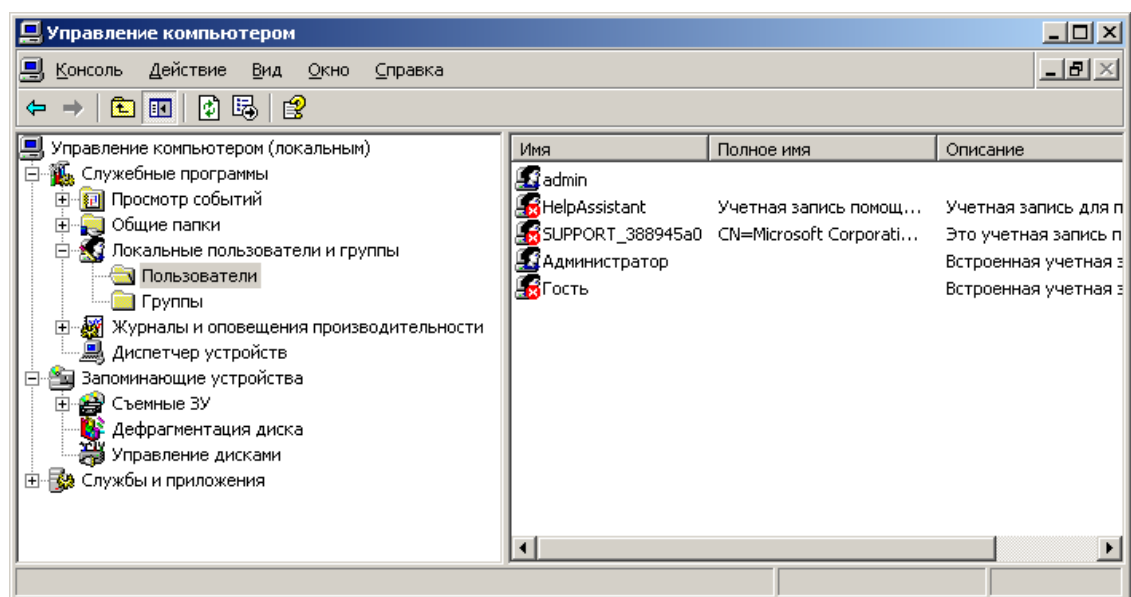


Рис. 1. Вікно оснащення Local Users and Groups у складі оснащення Computer Management.

Крім того, можуть з'явитися і інші призначені для користувача облікові записи, наприклад, після установки служб Інтернету – Internet Information Services.

Для роботи з локальними користувачами можна використовувати утиліту командного рядка net user.

<sup>1</sup> Обліковий запис HelpAssistant, що використовується в системах Windows XP при роботі засобу віддаленої допомоги Remote Assistance; у Windows Server 2003 відсутній.

## Папка Groups

У системах Windows 2000 (на робочій станції або сервері, що є членом домену) папка **Groups** (Групи) містить шість вбудованих груп, що створюються автоматично при установці системи:

- **Administrators** (Адміністратори) – її члени володіють повним доступом до всіх ресурсів системи. Це єдина вбудована група, що автоматично надає своїм членам весь набір вбудованих прав. За умовчанням містить вбудований обліковий запис Administrator. Якщо комп'ютер підключений до домену, ця група також містить групу Domain Admins.
- **Backup Operators** (Оператори архіву) – члени цієї групи можуть архівувати і відновлювати файли в системі незалежно від того, якими правами ці файли захищені. Крім того, оператори архіву можуть входити в систему і завершувати її роботу, але вони не мають права змінювати налаштування безпеки. За умовчанням порожня.
- **Guests** (Гості) – ця група дозволяє виконати реєстрацію користувача за допомогою облікового запису Guest і отримати обмежені права на доступ до ресурсів системи. Члени цієї групи можуть завершувати роботу системи. За умовчанням містить користувача Guest.
- **Power Users** (Досвідчені користувачі) – члени цієї групи можуть створювати облікові записи користувачів, але вони мають право модифікувати настройки безпеки тільки для створених ними облікових записів. Крім того, вони можуть створювати локальні групи і модифікувати склад членів створених ними груп. Те ж саме вони можуть робити з групами Users, Guests і Power Users. Члени групи Power Users не можуть модифікувати членство в групах Administrators і Backup Operators. Вони не можуть бути власниками файлів, архівувати або відновлювати каталоги, завантажувати і вивантажувати драйвери пристроїв і модифікувати налаштування безпеки і журнал подій. За умовчанням порожня.
- **Replicator** (Реплікатор) – членом групи Replicator повинен бути тільки обліковий запис, за допомогою якого можна реєструватися в службі реплікації контролера домену. Її членами не слід робити робочі облікові записи. За умовчанням порожня.
- **Users** (Користувачі) – члени цієї групи можуть виконувати більшість призначених для користувача функцій, наприклад, запускати додатки, користуватися локальним або мережним принтером, завершувати роботу системи або блокувати робочу станцію. Вони також можуть

створювати локальні групи і регулювати склад їх членів. Вони не можуть отримати доступ до загального каталогу або створити локальний принтер. За умовчанням містить службові облікові записи NT AUTHORITY\Authenticated Users (S-1-5-11) і NT AUTHORITY\INTERACTIVE (S-1-5-4). Якщо комп'ютер підключений до домену, ця група також містить групу Domain Users.

У системах Windows XP з'явилися ще три групи.

- **Network Configuration Operators** (Оператори настройки мережі) – група, члени якої мають деякі права по налаштуванню мережних служб і параметрів. За умовчанням порожня.
- **Remote Desktop Users** (Користувачі віддаленого робочого столу) – ця група містить імена користувачів, яким явно дозволений віддалений доступ до робочого столу.
- **Help Services Group** (Група служб підтримки) – група для підтримки довідкової служби Help and Support Service. За умовчанням містить обліковий запис SUPPORT\_388945a0.

Ще чотири групи з'явилися в системах Windows Server 2003.

- **Performance Log Users** – члени цієї групи можуть віддалено запускати журнали реєстрації. За умовчанням містить службовий обліковий запис NT\_AUTHORITY\NETWORK SERVICE (S-1-5-20).
- **Performance Monitor Users** – група, члени якої можуть виконувати моніторинг продуктивності комп'ютера. За умовчанням порожня.
- **Print Operators** – члени цієї групи можуть адмініструвати принтери в домені. За умовчанням порожня.
- **Telnet Clients** – група, члени якої мають доступ до служби Telnet Server на даному комп'ютері. За умовчанням порожня.

Для роботи з локальними групами можна використовувати утиліту командного рядка net localgroup.

### **Управління робочим середовищем користувача**

Робоче середовище користувача складається з налаштувань робочого столу, наприклад, кольору екрану, налаштувань миші, розміру і розташування вікон, з налаштувань процесу обміну інформацією по мережі і з пристроєм друку, змінних середовища, параметрів реєстру і набору доступних додатків.

Для управління середовищем користувача призначені наступні засоби систем Windows 2000/XP/2003.

- Профілі користувачів. У профілі користувача зберігаються всі налаштування робочого середовища системи, визначені самим

користувачем. Це можуть бути, наприклад, налаштування екрану і з'єднання з мережею. Всі налаштування, що виконуються самим користувачем, автоматично зберігаються в папці, ім'я якої для щойно встановленої системи виглядає таким чином: %SystemDrive%\Documents and Settings\%username%.

- Сценарій входу в систему (сценарій реєстрації) є командним файлом, що має розширення .bat або .cmd, виконуваним файлом з розширенням .exe або сценарієм VBScript, який запускається при кожній реєстрації користувача в системі або виході з неї. Сценарій може містити команди операційної системи, призначені, наприклад, для створення з'єднання з мережею або для запуску додатку. Крім того, за допомогою сценарію можна встановлювати значення змінних середовища, що вказують шляхи пошуку, каталоги для тимчасових файлів та іншу інформацію.
- Сервер сценаріїв Windows (Windows Scripting Host, WSH). Сервер сценаріїв незалежний від мови і призначений для роботи на 32-розрядних платформах Windows. Він включає як ядро сценаріїв Visual Basic Scripting Edition (VBScript), так і JScript. Сервер сценаріїв Windows призначений для виконання сценаріїв прямо на робочому столі Windows або у вікні консолі команд. При цьому сценарії не потрібно вбудовувати в документ HTML.

### **Профілі користувачів**

На ізольованому комп'ютері з Windows XP локальні профілі користувачів створюються автоматично. Інформація локальних профілів необхідна для підтримки налаштувань робочого столу локального комп'ютера, характерних для конкретного користувача. Профіль створюється для кожного користувача в процесі його першої реєстрації в комп'ютері.

Профіль користувача має наступні перевагами:

- при реєстрації користувача в системі робочий стіл одержує ті самі налаштування, які існували у момент попереднього виходу користувача з системи;
- декілька користувачів можуть працювати на одному і тому ж комп'ютері в індивідуальних середовищах (не можна тільки мати власні параметри роздільної здатності екрану і частоти розгортки; тут потрібно застосовувати профілі обладнання);
- при роботі комп'ютера в домені профілі користувачів можуть бути збережені на сервері. В цьому випадку користувач дістає можливість працювати зі своїм профілем при реєстрації на будь-якому комп'ютері мережі. Такі профілі називаються переміщуваними (roaming profile). Різновидом переміщуваних профілів є обов'язкові профілі (mandatory

profiles). Такий профіль користувач не може змінювати, і всі зміни, зроблені в налаштуваннях системи, втрачаються при виході з неї. У Windows XP і Windows Server 2003 обов'язкові профілі підтримуються тільки для сумісності, замість них рекомендується застосовувати групові політики.

### **Налаштування, що зберігаються в профілі користувача**

Профіль користувача зберігає налаштування конфігурації і параметри, що індивідуально призначаються кожному користувачу і що повністю визначають його робоче середовище (табл. 1).

Таблиця 1. Налаштування профілю користувача

<b>Об'єкт</b>	<b>Відповідні йому параметри</b>
Windows Explorer	Всі налаштування, визначені самим користувачем, що стосуються програми Windows Explorer
Панель завдань	Всі персональні групи програм і їх властивості, всі програмні об'єкти і їх властивості, всі налаштування панелі завдань
Налаштування принтера	Мережні з'єднання принтера
Панель управління	Всі налаштування, визначені самим користувачем, що стосуються панелі управління
Стандартні	Налаштування всіх стандартних додатків, що запускаються для конкретного користувача
Додатки, що працюють в операційній системі	Будь-який додаток, спеціально створений для роботи в середовищі Windows XP/2003, може володіти засобами відстеження своїх налаштувань щодо кожного користувача. Якщо така інформація існує, вона зберігається в профілі користувача
Електронна підказка	Будь-які закладки, встановлені в довідковій системі Windows
Консоль управління Microsoft	Індивідуальний файл конфігурації і поточного стану консолі управління

### **Структура нового профілю користувача**

Профіль користувача створюється на основі профілю, що призначається за умовчанням. Він зберігається на кожному комп'ютері, де працює Windows XP. Файл NTUSER.DAT, що знаходиться в папці Default User, містить налаштування конфігурації, що зберігаються в реєстрі Windows XP. Крім того, кожен профіль користувача використовує загальні програмні групи, що знаходяться в теці All Users.



## Структура профілю користувача

При створенні профілю користувача використовується профіль, що призначається за умовчанням, що знаходиться в папці Default User. Папка Default User, папки профілів індивідуальних користувачів, а також папки All Users, LocalService і NetworkService знаходяться в папці Documents and Settings кореневого каталогу на завантажувальному томі. У папці кожного користувача знаходяться файл NTUSER.DAT і список посилань на об'єкти робочого столу. На рис. 2 показана структура тек локального профілю користувача. У цих папках, зокрема, зберігаються посилання на різні об'єкти робочого столу. Файл ntuser.dat.LOG є журналом транзакцій, що фіксує зміни профілю і дозволяє відновити його у разі, коли відбувається пошкодження файлу NTUSER.DAT.

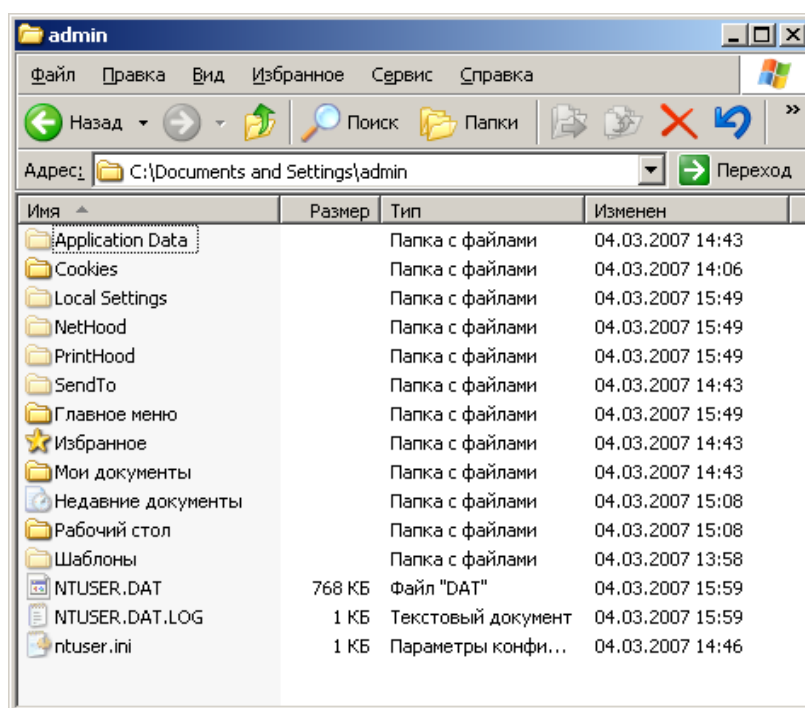


Рис. 2. Структура підпапок профілю користувача.

У табл. 2 перераховані підпапки, що знаходяться усередині папки локального профілю користувача, і описано їх вміст. Деякі з цих підпапок є прихованими і можуть бути не видні при звичайному перегляді. Всі вказані папки, окрім Local Settings, входять в переміщуваний профіль користувача (при роботі комп'ютера у складі домену). При використанні звичайного профілю локальні папки Application Data, Desktop, My Documents, My Pictures і Start Menu можна перепризначувати на спільні мережні диски за допомогою оснащення-розширення Folder Redirection (Перенаправлення папки), що входить в оснащення Group Policy Object Editor (Групова політика).

Таблиця 2. Вміст папки локального профілю користувача

Підпапка	Вміст
Application Data	Дані, що відносяться до конкретних додатків, наприклад, індивідуальний словник. Розробники додатків самі вирішують, які дані повинні бути збережені в папці профілю користувача
Cookies	Службові файли, отримані з перегляду веб-серверів
Desktop (Робочий стіл)	Об'єкти робочого столу, включаючи файли і ярлики
Favorites (Вибране)	Ярлики часто використовуваних програм і папок
Local Settings	Дані про локальні налаштування, що впливають на роботу програмного забезпечення комп'ютера
My Documents (Мої документи)	Дані про документи і графічні файли, що використовуються користувачем
My Recent Documents (Документи, що недавно використалися)	Дані про документи і графічні файли, відкриті користувачем останнім часом
NetHood	Ярлики об'єктів мережного оточення
PrintHood	Ярлики об'єктів папки принтера
Recent	Ярлики недавно використовуваних об'єктів
SendTo	Ярлики об'єктів, куди можуть надсилатися документи
Start Menu (Головне меню)	Ярлики програм
Templates (Шаблони)	Ярлики шаблонів
UserData	Службова інформація

Для управління профілями користувача є більше десятка групових політик, які доступні у вікні оснащення **Group Policy Object Editor** в розділах Computer Configuration | Administrative Templates | System | User Profiles та User Configuration | Administrative Templates | System | User Profiles.

## Завдання до виконання роботи

1. За допомогою аплету "Учетные записи пользователей" (рис. 3) панелі управління (**Пуск | Настройка | Панель управления | Учетные записи пользователей**) створити користувача з обмеженими та адміністративними правами. Змінити користувачам рисунки, що відображаються на екрані привітання при вході в систему (рис. 4). Змінити паролі користувачам (звернути увагу на попередження системи при зміні паролю чужого облікового запису). Видалити один зі створених облікових записів користувача.

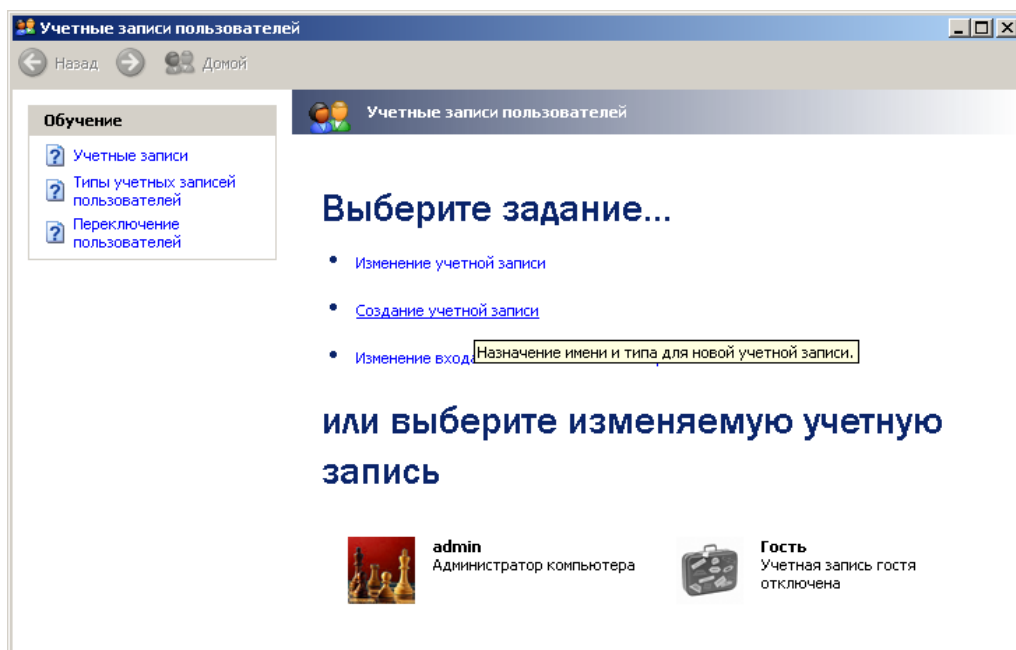


Рис. 3. Аплет "Учетные записи пользователей" панелі управління.

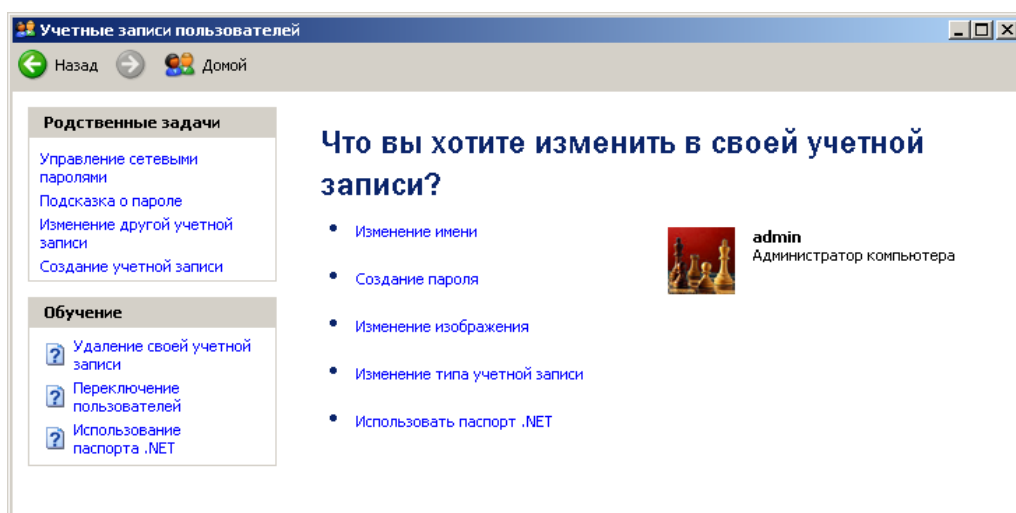


Рис. 4. Зміна налаштувань облікового запису за допомогою панелі управління.

2. За допомогою аплету "Учетные записи пользователей" панелі управління створити для свого облікового запису дискету скидання пароля, яка дозволить коректно змінити пароль у випадку його втрати та увійти в систему (рис. 5). Для створення такої дискети вибирають пункт "Подсказка о пароле" меню "Родственные задачи" (рис. 5) і слідують інструкціям майстра (рис. 6).

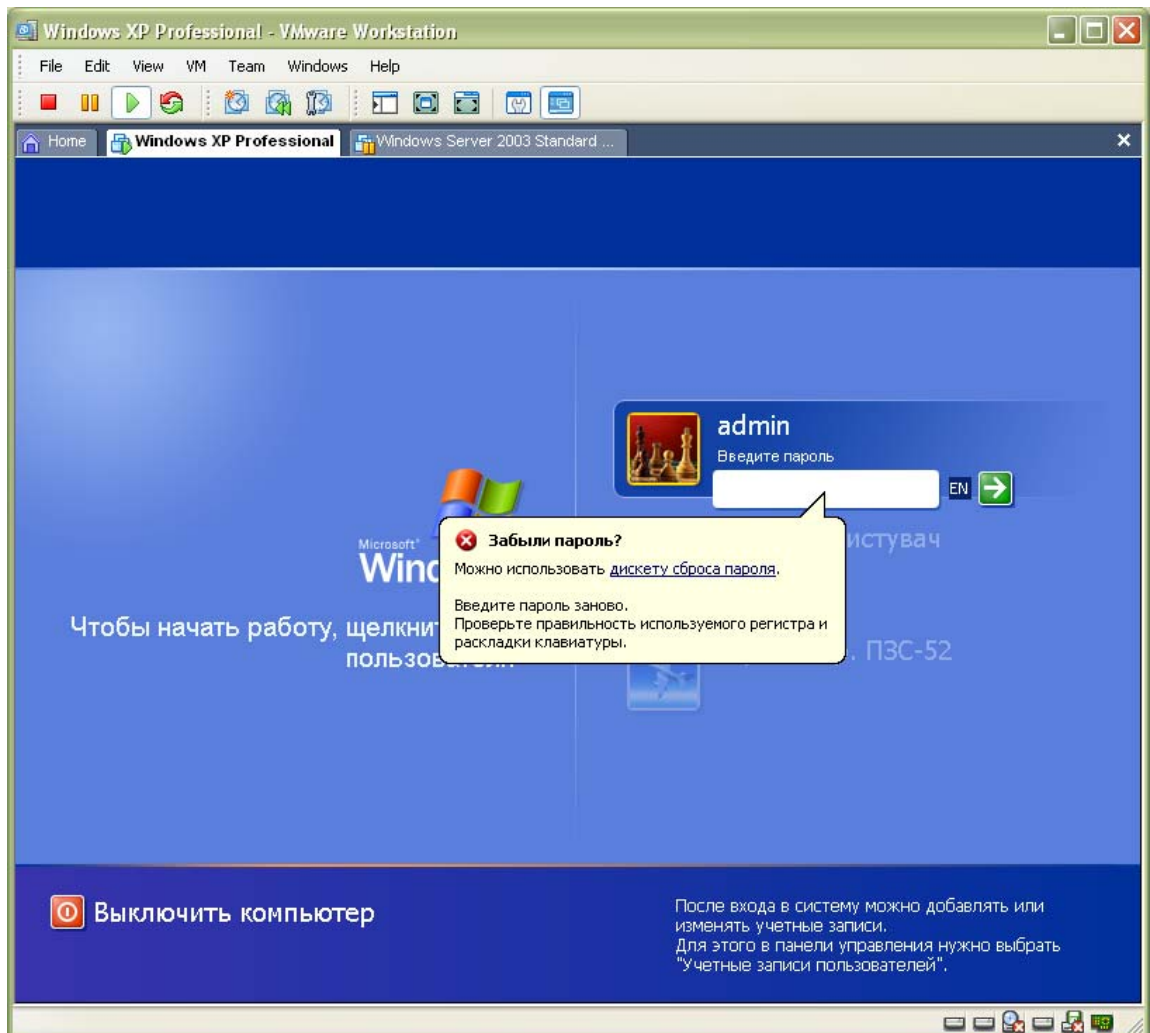


Рис. 5. Ілюстрація роботи дискети скидання пароля.

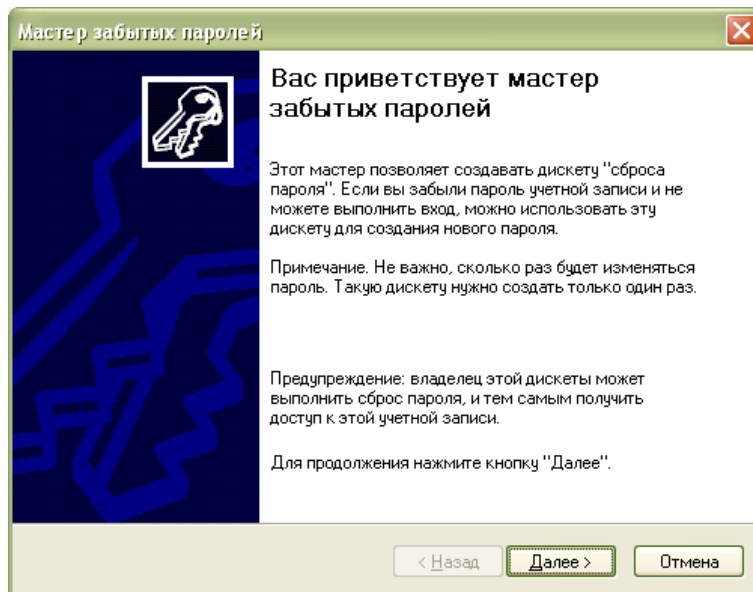


Рис. 6. Створення дискети скидання пароля.

3. За допомогою оснастки "Локальные пользователи и группы" консолі mms створити користувача, призначити йому початковий пароль та поставити вимогу зміни пароля при наступному вході в систему (рис. 7).

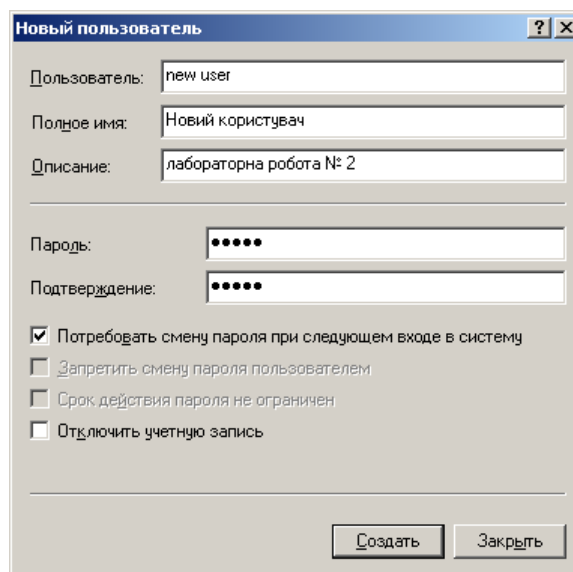


Рис. 7. Створення нового облікового запису за допомогою оснащення mms.

4. За допомогою оснастки "Локальные пользователи и группы" консолі mms внести створеного користувача в групу "Операторы архива" (рис. 8). Створити нову групу та внести в неї цього ж користувача (рис. 9).

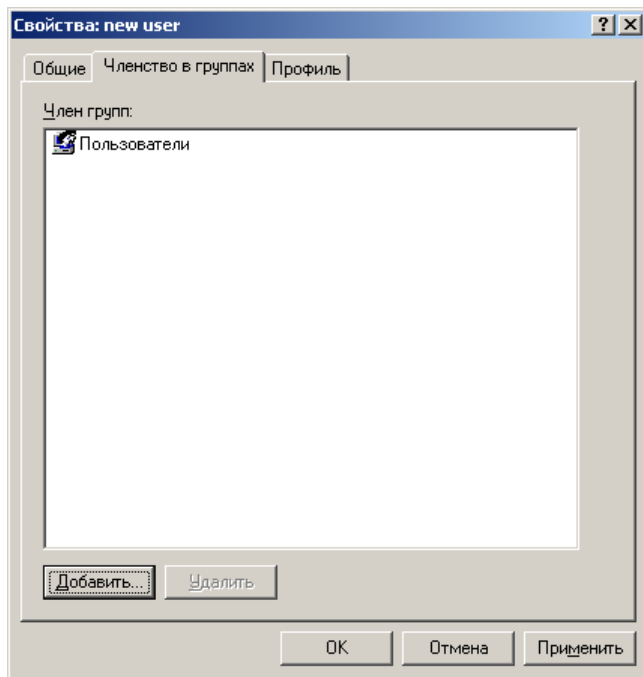


Рис. 8. Вивід відомостей про членство облікового запису в групах.

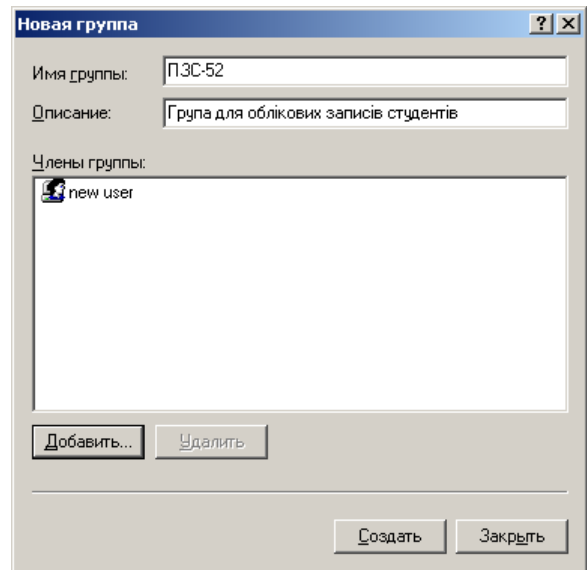


Рис. 9. Створення нової локальної групи.

5. За допомогою утиліти командного рядка *net user* створити користувача (довідка по цій утиліті викликається за допомогою команди *net help user* або *net user /?*) з обмеженим терміном дії облікового запису (місяць) та з дозволом входити в систему тільки з 8:00 до 17:00 в робочі дні (рис. 10, 11). Змінити системну дату/час на вихідний день/неробочий час (17:00–08:00) та перевірити можливість входу цього користувача в систему. Змінити системну дату на більш ніж місяць вперед та перевірити можливість входу цього користувача в систему.

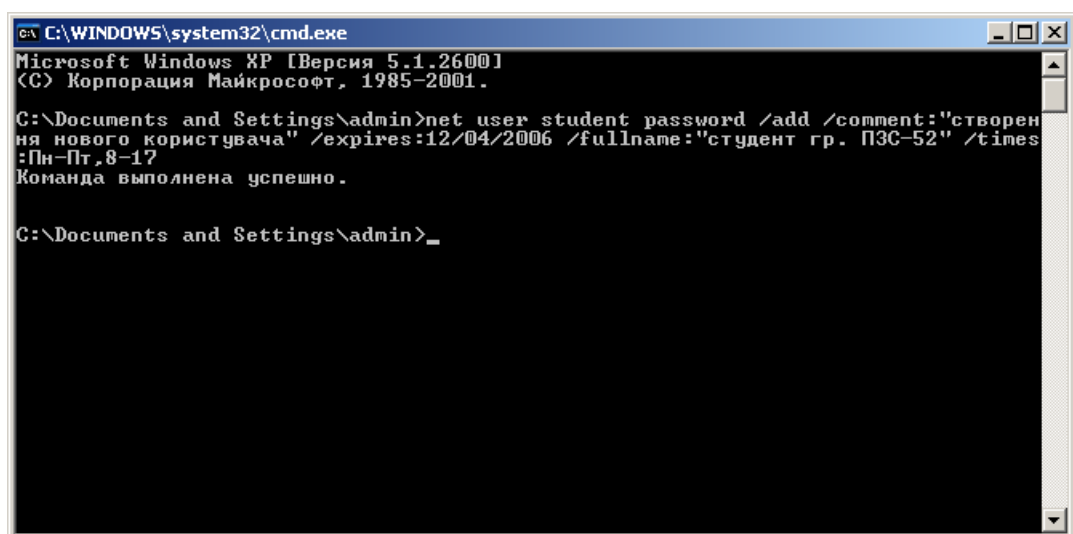


Рис. 10. Управління користувачами за допомогою командного рядка.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\admin>net user student
Имя пользователя      student
Полное имя            студент гр. ПЗС-52
Комментарий           створення нового користувача
Код страны            000 <Стандартный системный>
Учетная запись активна Yes
Учетная запись просрочена 4/12/2006 12:00 AM

Последний пароль задан 3/12/2006 3:56 PM
Действие пароля завершается 4/24/2006 2:43 PM
Пароль допускает изменение 3/12/2006 3:56 PM
Требуется пароль      Yes
Пользователь может изменить пароль Yes

Разрешенные рабочие станции Все
Сценарий входа
Конфигурация пользователя
Основной каталог
Последний вход        3/13/2006 3:58 PM

Разрешенные часы входа Monday 8:00 AM - 5:00 PM
Tuesday 8:00 AM - 5:00 PM
Wednesday 8:00 AM - 5:00 PM
Thursday 8:00 AM - 5:00 PM
Friday 8:00 AM - 5:00 PM

Членство в локальных группах *Пользователи
Членство в глобальных группах *Отсутствует
Команда выполнена успешно.

C:\Documents and Settings\admin>
```

Рис. 11. Вивід відомостей про обліковий запис за допомогою командного рядка.

6. За допомогою утиліти командного рядка *net localgroup* створити нову групу та внести в неї користувача (довідка по цій утиліті викликається за допомогою команди *net help localgroup* або *net localgroup /?*), вивести відомості про цю групу на екран (рис. 12, 13).

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\admin>net localgroup STUDENTS /comment:"локальна група
для студентів каф. ПЗ" /add
Команда выполнена успешно.

C:\Documents and Settings\admin>net localgroup STUDENTS student /add
Команда выполнена успешно.

C:\Documents and Settings\admin>net localgroup STUDENTS
Имя псевдонима      STUDENTS
Комментарий         локальна група для студентів каф. ПЗ

Члены
-----
student
Команда выполнена успешно.

C:\Documents and Settings\admin>
```

Рис. 12. Управління локальними групами за допомогою командного рядка.

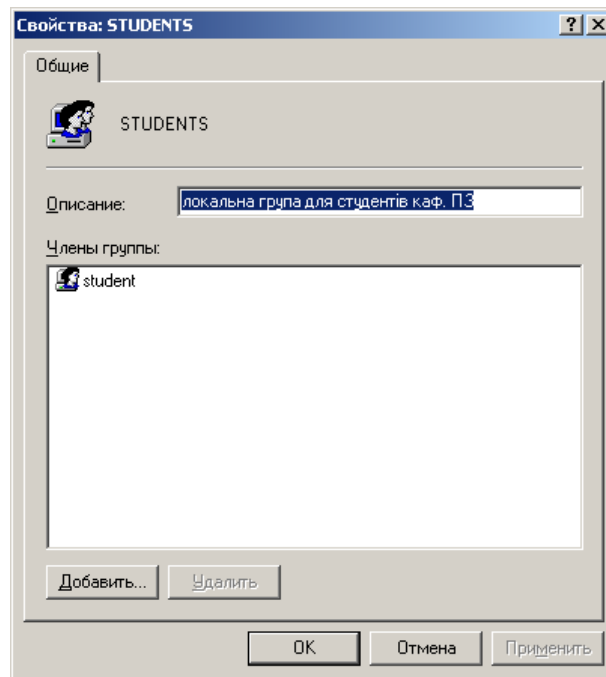


Рис. 13. Властивості групи користувачів в оснащенні mmc.

7. Створити новому користувачу переміщуваний профіль. Для цього попередньо налаштований профіль тестового користувача копіюється в нову папку (наприклад на інший том або ж на інший комп'ютер в мережі): **Мой компьютер | Свойства | Дополнительно | Профили пользователей: Параметры | Копировать** (рис. 14); у вікні, що з'явиться вказують шлях копіювання та дозволи на використання профілю (рис. 15).

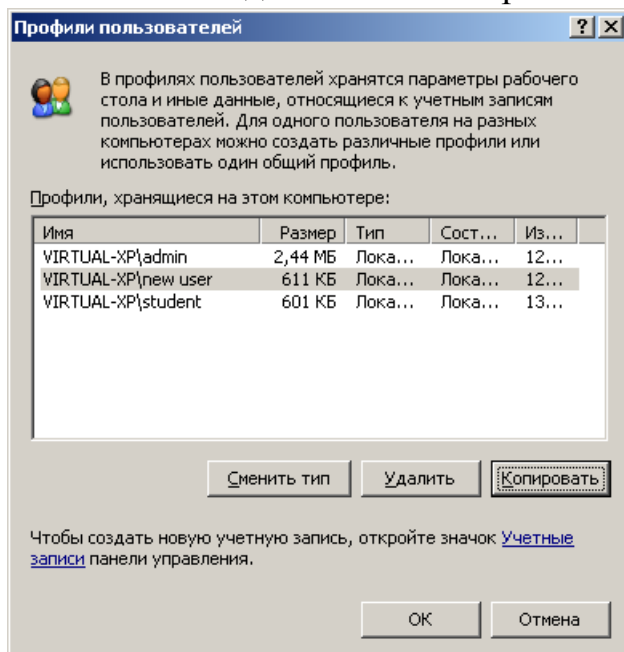


Рис. 14. Вікно профілів користувачів у властивостях комп'ютера.

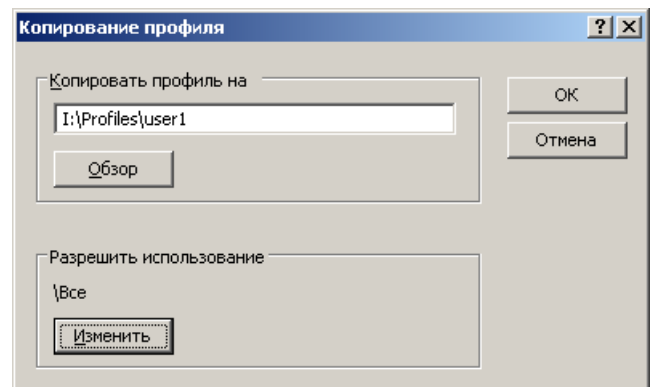


Рис. 15. Копіювання профілю користувача.



Після створення папки з профілем необхідно зробити відповідні налаштування у властивостях облікового запису користувача (рис. 16). Якщо необхідно, щоб при вході користувача в систему виконувались певні команди / програми, тут же можна прописати сценарій входу (зверніть увагу: файл сценарію повинен розміщуватись в папці %systemroot%\system32\repl\Import\Scripts; якщо такого шляху не існує, його треба створити).

Увійти в систему під користувачем, для якого робились налаштування, переконатись у правильності виконаних дій.

Зробити профіль цього користувача обов'язковим: для цього слід перейменувати файл ntuser.dat в папці профілю у файл ntuser.man. Увійти в систему під цим користувачем, переконатись, що зміни налаштувань не зберігаються при виході користувача з системи.

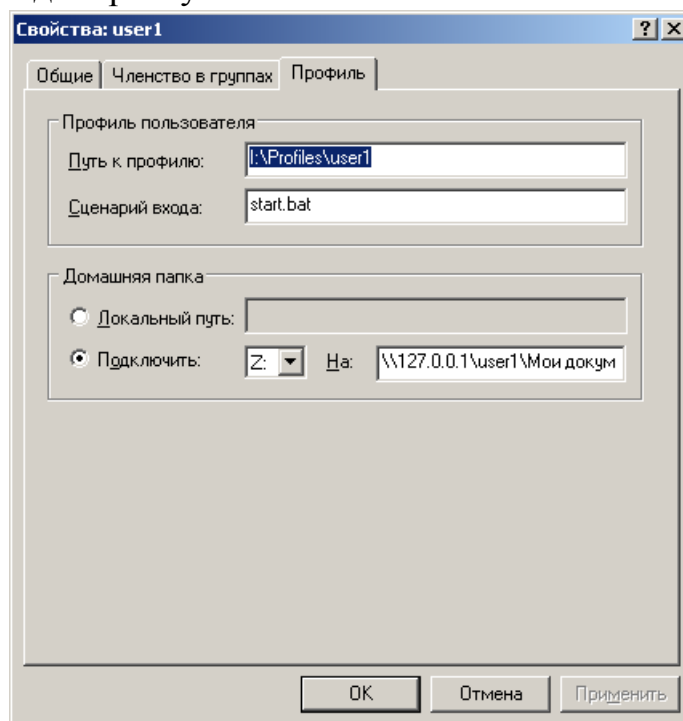


Рис. 16. Налаштування переміщеного профілю користувача.

### Контрольні запитання.

1. Які користувачі створюються автоматично при інсталяції системи Windows XP?
2. Як в Windows XP користувач може змінити свій пароль?
3. Що таке профіль користувача, що таке обов'язковий профіль?
4. Призначення груп користувачів в Windows XP, вбудовані групи.
5. Як в Windows XP зробити обліковий запис користувача, що дійсний протягом певного періоду часу?

## **Лабораторна робота № 2.**

### **ДОЗВОЛИ ТА КВОТИ NTFS. ШИФРУВАННЯ ФАЙЛІВ: EFS.**

**Мета роботи:** Навчитись ефективно налагоджувати систему логічного розділення доступу до об'єктів файлової системи в ОС Windows XP Professional; управляти квотами на томах NTFS та використовувати шифровану файлову систему EFS.

#### **Теоретичні відомості.**

##### **Права доступу (дозволи) для файлів і каталогів**

Встановлюючи користувачам певні дозволи на доступ до файлів і каталогів (папок), адміністратори системи можуть захищати конфіденційну інформацію від несанкціонованого доступу. Кожен користувач має певний набір дозволів на доступ до кожного об'єкту файлової системи.

Крім того, користувач може бути власником файлу або папки, якщо сам їх створює. Питання передачі права володіння розглядається нижче.

Дозволи користувача на доступ до об'єктів файлової системи працюють за принципом доповнення (адитивності). Це значить, що діючі дозволи, тобто ті дозволи, які користувач реально має відносно конкретного каталогу або файлу, утворюються зі всіх прямих і непрямих дозволів, призначених користувачу для цього об'єкту за допомогою логічної функції АБО. Наприклад, якщо користувач має прямо призначений дозвіл для каталогу на читання, а опосередковано через членство в групі йому дано дозвіл на запис, то в результаті користувач зможе читати інформацію у файлах каталогу і записувати в них дані.

Слід зазначити, що правило додавання дозволів за допомогою логічного АБО не виконується, коли користувач має певний дозвіл, а групі, в яку він входить, відмовлено в цьому дозволі (або навпаки). В цьому випадку відмова в дозволі (Deny) має вищий пріоритет над наданням дозволу, тобто в результаті користувач не матиме цього дозволу. Поява можливості відмови користувачу або групі в дозволі для файлів і каталогів зробила непотрібним дозвіл No Access, що застосовувався в Windows NT 4.0. Тепер для відмови користувачу в дозволі на доступ до якого-небудь файлу або каталогу слід включити користувача в групу, якій відмовлено в дозволі Full Control (Повний доступ) для даного об'єкту файлової системи<sup>1</sup>.

---

<sup>1</sup> Нагадаємо, що дозволи підтримуються тільки на файловій системі NTFS, тому не дивуйтеся, якщо ви не побачите вкладку Security (Безпека) у властивостях дискових томів, що відформатовані для FAT або FAT32.

Кожен зі стандартних дозволів складається з набору спеціальних (особливих) дозволів, що задають можливість виконання тієї або іншої дії з файлами або каталогами. У табл. 3 показано відповідність стандартних і спеціальних дозволів для файлів і каталогів. Детальний опис спеціальних дозволів наведено в табл. 4.

Таблиця 3 Відповідність стандартних і спеціальних дозволів

Спеціальні дозволи	Стандартні дозволи					
	Full Control	Modify	Read & Execute	List Folder Contents	Read	Write
<b>Traverse Folder/Execute File</b> (Огляд папок/ Виконання файлів)	+	+	+	+		
<b>List Folder/Read Data</b> (Зміст папок/ Читання даних)	+	+	+	+	+	
<b>Read Attributes</b> (Читання атрибутів)	+	+	+	+	+	
<b>Read Extended Attributes</b> (Читання додаткових атрибутів)	+	+	+	+	+	
<b>Creat Files/Write Data</b> (Створення файлів/Запис даних)	+	+				+
<b>Create Folders/Append Data</b> (Створення папок/ Дозапис даних)	+	+				+
<b>Write Attributes</b> (Запис атрибутів)	+	+				+
<b>Write Extended Attributes</b> (Запис додаткових атрибутів)	+	+				+
<b>Delete Subfolders and Files</b> (Видалення підпапок і файлів)	+					
<b>Delete</b> (Видалення)	+	+				
<b>Read Permissions</b> (Читання дозволів)	+	+	+	+	+	+
<b>Change Permissions</b> (Зміна дозволів)	+					

<b>Take Ownership</b> (Зміна власника)	+					
--	---	--	--	--	--	--

Хоча дозволи "List Folder Contents" ("Список вмісту папки") і "Read & Execute" ("Читання і виконання") включають одні і ті ж спеціальні дозволи, вони успадковуються по-різному. Дозвіл "List Folder Contents" успадковується тільки каталогами, але не файлами, і відображається тільки при перегляді дозволів на доступ до папок. Дозвіл "Read & Execute" успадковується як файлами, так і папками, і завжди відображається при перегляді дозволів на доступ до файлів або папок.

Таблиця 4. Спеціальні дозволи для файлів і каталогів

Спеціальний дозвіл	Опис
<b>Traverse Folder / Execute File</b>	Визначає можливість переміщення по каталогах файлової системи незалежно від того, має або не має користувач дозволу для перегляду каталогів, що перетинаються в процесі переміщення. На роботу цього дозволу впливає політика безпеки Bypass Traverse Checking (Обхід перехресної перевірки) (див. вузол <b>Local Policies   User Rights Assignment</b> в параметрах безпеки). Дозвіл Execute File (Виконання файлів) визначає можливість виконання програм.
<b>List Folder / Read Data</b>	Визначає можливість перегляду імен файлів або підкаталогів даного каталогу (відноситься тільки до каталогу). Дозвіл Read Data (Читання даних) визначає можливість перегляду вмісту файлу.
<b>Read Attributes</b>	Визначає можливість перегляду атрибутів файлу або каталогу. Самі атрибути визначаються операційною системою.
<b>Read Extended Attributes</b>	Визначає можливість перегляду додаткових атрибутів файлу або каталогу. Самі додаткові атрибути визначаються операційною системою.
<b>Create Files / Write Data</b>	Визначає можливість створення файлів усередині каталогу (відноситься тільки до каталогів). Дозвіл Write Data (Запис даних) визначає можливість зміни вмісту файлів або перезапису існуючих даних файлу новою інформацією (відноситься тільки до файлів).
<b>Create Folders / Append Data</b>	Визначає можливість створювати підкаталоги усередині даного каталогу (відноситься тільки до каталогів). Дозвіл Append Data (Дозапис даних) визначає можливість приєднання нових даних до існуючого файлу без зміни, знищення або перезапису існуючої інформації (відноситься тільки до файлів).

<b>Write Attributes</b>	Визначає можливість зміни атрибутів файлу або каталогу. Атрибути визначаються операційною системою.
<b>Write Extended Attributes</b>	Визначає можливість зміни додаткових атрибутів файлу або каталогу. Додаткові атрибути визначаються програмою і можуть бути нею змінені.
<b>Delete Subfolders and Files</b>	Визначає можливість видалення підкаталогів і файлів, що знаходяться в даному каталозі, навіть якщо для цих підкаталогів і файлів немає дозволу Delete (Видалення). Цей дозвіл є тільки у каталогів.
<b>Delete</b>	Визначає можливість видалення файлу або каталогу. Якщо вам відмовлено в дозволі Delete (Видалення) для даного каталогу або файлу, ви все ж таки можете видалити їх, одержавши дозвіл Delete Subfolders and Files (Видалення підпапок і файлів) на батьківський каталог.
<b>Read Permissions</b>	Визначає можливість читання дозволів для файлів і каталогів, таких як Full Access, Read і т.д.
<b>Change Permissions</b>	Визначає можливість зміни дозволів для файлів і каталогів, таких як Full Access, Read і т.д.
<b>Take Ownership</b>	Визначає можливість взяття у власність даного файлу або каталогу. Власник файлу або каталогу може завжди змінити дозволи до цього об'єкту, незалежно від інших дозволів.

### **Визначення діючих дозволів для файлів і папок**

Як вже зазначалось, користувач або група одержують дозволи на доступ до файлів або папок безпосередньо і через членство в групах (в доменах Windows 2000 і Windows Server 2003 групи можуть бути членами інших груп). Тому, коли виникає питання "а які ж врешті-решт права має даний користувач?" відповідь одержати не так просто і швидко. Системи Windows XP Professional і Windows Server 2003 пропонують нову можливість – визначення діючих дозволів (effective permissions).

При визначенні дозволів, що діють, потрібно пам'ятати про те, що користувач може мати права на операції з об'єктом, призначені не за допомогою механізму дозволів, а через політики безпеки. Наприклад, користувач може змінювати власника об'єкту, навіть якщо у нього немає дозволу Take Ownership, проте якщо таке право йому дане в політиках безпеки.

### **Квоти дискового простору**

Адміністрування великих комп'ютерних мереж, де сервери підтримують роботу сотень користувачів, зв'язане з рядом складнощів. Одна з них – облік дискового простору серверу, зайнятого файлами співробітників компанії. Як

правило, користувачі, що зберігають свої файли на сервері, мало піклуються про актуальність інформації і про знищення застарілих або непотрібних даних. Безліч тимчасових файлів і копій одного й того ж файлу, що знаходяться в різних папках, лише посилюють ситуацію. В результаті в лічені місяці навіть на великих жорстких дисках серверу може не виявитися необхідного для роботи вільного простору.

Як правило, у великих організаціях дерево каталогів вельми розгалужене, тому візуальний контроль витрачання дискового простору користувачами віднімає у адміністраторів багато часу і зусиль.

Подібна проблема просто розв'язується за допомогою введення квот на дисковий простір, доступний для роботи кожному користувачу. У попередніх версіях операційної системи Windows NT не було штатних можливостей ввести квоту на доступний дисковий простір, тому будь-який користувач міг розпоряджатися усім простором жорстких дисків комп'ютера. У Windows 2000/XP і Windows Server 2003 адміністратор може квотувати дисковий простір по **кожному тому** і для **кожного користувача**. (З цього випливає, що неможливо задати квоту для окремих каталогів або груп.)

Система враховує загальний простір, зайнятий файлами, власником яких є контрольований користувач: якщо користувач володіє файлом, розмір останнього додається до загальної суми зайнятого користувачем дискового простору. Важливо відзначити, що, оскільки квотування виконується на рівні тому, не має значення, чи знаходиться том на одному фізичному жорсткому диску або на різних пристроях. І навпаки, якщо на одному фізичному диску зберігається декілька томів, то квотування може здійснюватися індивідуально по кожному тому.

Після установки квот дискового простору користувач зможе зберігати на томі обмежений об'єм даних, тоді як на цьому томі може залишатися вільний простір. Якщо користувач перевищує видану йому квоту, в журнал подій вноситься відповідний запис. Потім, залежно від конфігурації системи, користувач або зможе записати інформацію на том ("м'який" режим обмежень), або йому буде відмовлено в записі через відсутність вільного простору ("жорсткий" режим).

Квоти можна використовувати на локальних і спільних мережних дисках (в цьому випадку загальний доступ повинен бути дозволений на рівні кореневого каталогу тому). Стиснення файлів не має значення при обчисленні зайнятого простору – завжди враховується розмір початкового нестиснутого файлу.

Встановлювати і проглядати<sup>1</sup> квоти на диску можна тільки в розділі з NTFS 5.0 і за наявності необхідних повноважень (що задаються за допомогою локальних або доменних групових політик) у користувача, що встановлює квоти. За умовчанням для роботи з квотами потрібно бути членом групи Administrators.

### **Передача права володіння**

У попередніх версіях Windows NT право володіння файлом або папкою було характеристикою, жорстко прив'язаною до творця даного об'єкту. Користувач, що створив файл або каталог, ставав власником цього об'єкту. Право володіння не могло бути передане іншому користувачу. Єдине виключення складав адміністратор, який міг стати власником об'єкту. Сам користувач не міг передати право володіння папкою або файлом іншому користувачу.

Операційні системи Windows 2000/XP і Windows Server 2003 забезпечують гнучкіше користування таким засобом забезпечення безпеки інформації, як право володіння об'єктом файлової системи. Тепер адміністратор або уповноважений користувач може призначити будь-якого користувача власником якого-небудь об'єкту файлової системи (ця можливість є тільки в Windows Server 2003) або користувач сам може стати власником об'єкту, не створеного ним самим. Природно, що для цього він повинен мати необхідні дозволи (Take Ownership). Крім того, за допомогою локальних або доменних політик безпеки можна вказувати, які користувачі завжди можуть ставати власниками файлів або інших об'єктів (за умовчанням таке право мають тільки адміністратори), при цьому вони можуть навіть не мати ніяких дозволів для цього об'єкту<sup>2</sup>.

Для передачі володіння об'єктом файлової системи або для прогляду поточного власника файлу або папки слід відкрити відповідне вікно властивостей, перейти на вкладку **Security**, потім натиснути кнопку **Advanced**. З'явиться вікно **Advanced Security Settings**. Перейдіть на вкладку **Owner** (Власник) цього вікна (рис. 17).

---

<sup>1</sup> У Windows XP і Windows Server 2003 для виконання будь-яких операцій з квотами можна також використовувати утиліту командного рядка Fsutil.exe.

<sup>2</sup> З вищесказаного випливає принцип відновлення дозволів для будь-якого об'єкту (зокрема для об'єктів, у яких помилково видалені всі дозволи): потрібно стати його власником, а потім встановити потрібні дозволи для інших користувачів і груп.

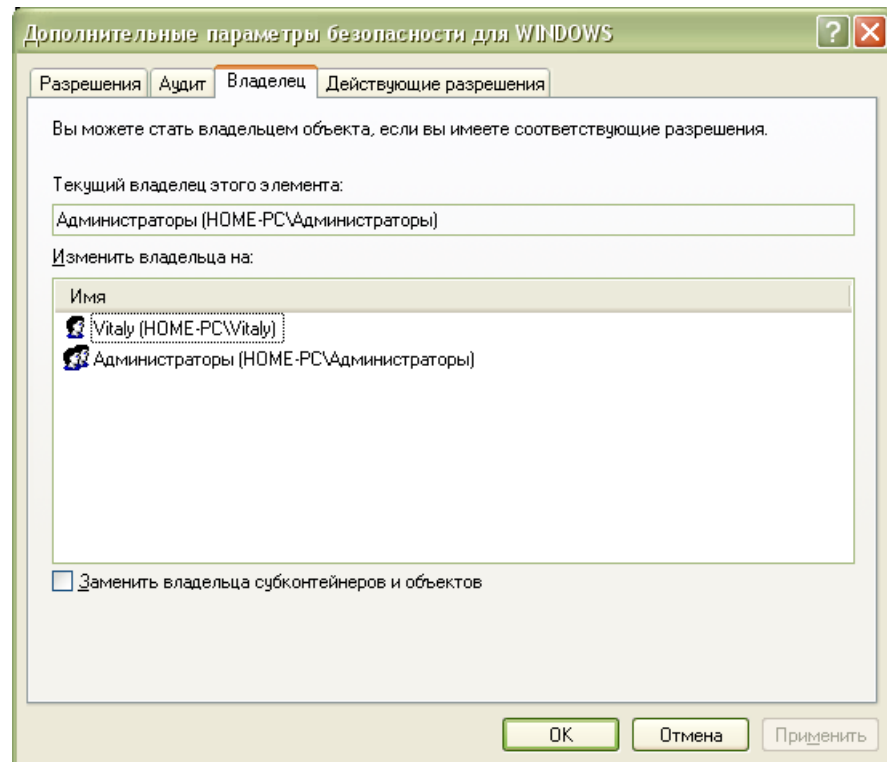


Рис.17. Вкладка Owner діалогового вікна Advanced Security Settings

У Windows Server 2003 адміністратор або інший користувач, що отримав (через відповідну політику безпеки) право зміни власників об'єктів, може натиснути кнопку **Other Users or Groups** (Інші користувачі або групи) і вибрати користувача (або групу), якого він хоче призначити власником об'єкту.

### Шифруюча файлова система EFS

На персональному комп'ютері операційну систему можна завантажити не з жорсткого, а з гнучкого чи компакт диска. Це дозволяє обійти проблеми, пов'язані з відмовою жорсткого диска і руйнуванням завантажувальних розділів. Проте, оскільки за допомогою змінного носія можна завантажувати різні операційні системи, будь-який користувач, що одержав фізичний доступ до комп'ютера, може обійти вбудовану систему управління доступом файлової системи NTFS і за допомогою певних інструментів прочитати інформацію жорсткого диска.

Єдиний надійний спосіб захисту інформації – це шифруюча файлова система. На ринку програмного забезпечення існує цілий набір продуктів, що забезпечують шифрування даних за допомогою утвореного від пароля ключа на рівні додатків. Проте такий підхід має ряд обмежень.

- Ручне шифрування і дешифрування. Служби шифрування більшості продуктів непрозорі для користувачів. Користувачу доводиться розшифровувати файл перед кожним його використанням, а потім



знову зашифровувати. Якщо користувач забуває зашифрувати файл після закінчення роботи з ним, інформація залишається незахищеною. Оскільки кожного разу необхідно вказувати, який файл повинен бути зашифрований (і розшифрований), застосування такого методу захисту інформації сильно утруднене.

- Просочування інформації з тимчасових файлів і файлів підкачки. Практично всі додатки в процесі редагування документів створюють тимчасові файли. Вони залишаються на диску незашифрованими, не зважаючи на те, що оригінальний файл зашифрований. Крім того, шифрування інформації на рівні додатків виконується в режимі користувача. Це значить, що ключ, вживаний для такого типу шифрування, може зберігатися у файлі підкачки. В результаті, за допомогою вивчення вмісту файлу підкачки можна одержати ключ і розшифрувати всі документи користувача.
- Слабка криптостійкість ключів. Ключі утворюються від паролів або випадкових фраз. Тому у випадку, якщо пароль легко запам'ятовується, атаки за допомогою словників можуть привести до швидкого злому системи захисту.
- Неможливість відновлення даних. Більшість продуктів, що дозволяють шифрувати інформацію, не надають засобів відновлення даних, що для користувачів є додатковим мотивом не застосовувати засоби шифрування. Це особливо стосується тих працівників, які не хочуть запам'ятовувати додатковий пароль. З другого боку, засіб відновлення даних за допомогою пароля – ще одна прогалина в системі захисту інформації. Все, що необхідно зловмиснику, – це пароль, призначений для запуску механізму відновлення даних, який дозволить отримати доступ до зашифрованих файлів.

Всі перераховані вище проблеми дозволяє вирішити шифруюча файлова система (Encrypting File System, EFS), вперше реалізована у Windows 2000, яка працює тільки на NTFS 5.0.

EFS містить наступні компоненти операційної системи (рис. 18):

- Драйвер EFS. Драйвер EFS є надбудовою над файловою системою NTFS. Він обмінюється даними зі службою EFS – запитує ключі шифрування, набори DDF (Data Decryption Field) і DRF (Data Recovery Field), – а також з іншими службами управління ключами. Одержану інформацію драйвер EFS передає бібліотеці реального часу файлової системи EFS (File System Run-Time Library, FSRTL), яка прозора для операційної системи виконує різні операції, характерні для файлової системи (читання, запис, відкриття файлу, приєднання інформації).

- Бібліотека реального часу файлової системи EFS. FSRTL – це модуль, який знаходиться усередині драйвера EFS і реалізовує виклики NTFS, що виконують такі операції, як читання, запис і відкриття зашифрованих файлів і каталогів, а також операції, пов'язані з шифруванням, дешифруванням і відновленням файлів при їх читанні або запису на диск. Хоча драйвери EFS і FSRTL реалізовані у вигляді одного компонента, вони ніколи не обмінюються даними безпосередньо. Для передачі повідомлень один одному вони використовують механізм викликів (callouts) NTFS, призначений для управління файлами. Це гарантує, що вся робота з файлами відбувається за безпосередньої участі NTFS.

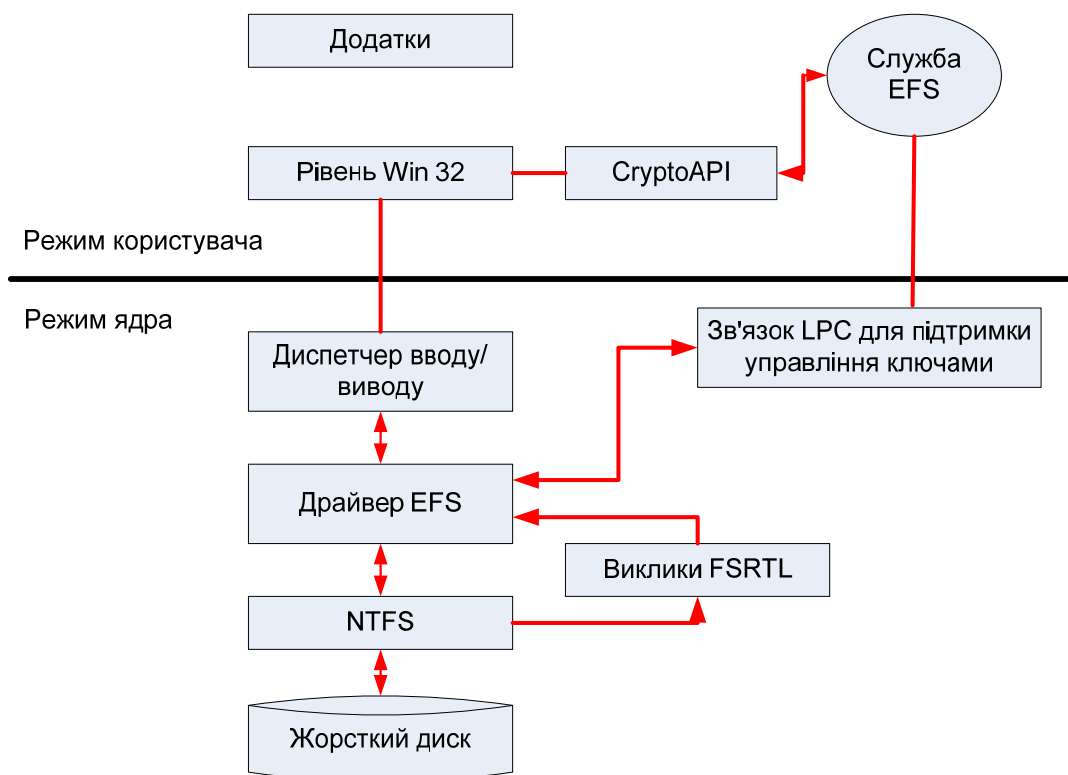


Рис. 18. Архітектура EFS

- Служба EFS. Служба EFS (EFS Service) є частиною системи безпеки операційної системи. Для обміну даними з драйвером EFS вона використовує порт зв'язку LPC, що існує між локальним адміністратором безпеки (Local Security Authority, LSA) і монітором безпеки, що працює в привілейованому режимі. У режимі користувача для створення ключів шифрування файлів і генерування даних для DDF і DRF служба EFS використовує CryptoAPI. Вона також підтримує набір API для Win32.

- Набір API для Win32. Цей набір інтерфейсів прикладного програмування дозволяє виконувати шифрування файлів, дешифровку і відновлення зашифрованих файлів, а також їх імпорт і експорт (без попередньої дешифровки). Ці API підтримуються стандартним системним модулем DLL – advapi32.dll.

EFS заснована на шифруванні з відкритим ключем і використовує всі можливості архітектури CryptoAPI. Кожен файл шифрується за допомогою випадково генерованого ключа, залежного від пари відкритого (public) і приватного (private) ключів користувача. Подібний підхід значною мірою утруднює здійснення великого набору атак, заснованих на криптоаналізі. При криптозахисті файлів може бути застосований будь-який алгоритм симетричного шифрування. EFS дозволяє здійснювати шифрування і дешифрування файлів, що знаходяться на віддалених файлових серверах.

Дані зашифровуються за допомогою симетричного алгоритму із застосуванням ключа шифрування файлу (File Encryption Key, FEK). FEK – це генерований випадковим чином ключ певної довжини. Своєю чергою, FEK шифрується за допомогою одного або декількох відкритих ключів, призначених для криптозахисту ключа. В цьому випадку створюється список зашифрованих ключів FEK, що дозволяє організувати доступ до файлу декільком користувачам. Для шифрування набору FEK використовується відкрита частина пари ключів кожного користувача. Список зашифрованих ключів FEK зберігається разом із зашифрованим файлом в спеціальному атрибуті EFS, званому полем дешифрування даних (Data Decryption Field, DDF). Інформація, необхідна для дешифрування, прив'язується до самого файлу. Приватна частина ключа користувача використовується при дешифруванні FEK. Вона зберігається в безпечному місці, наприклад на смарт-карті або іншому пристрої, що має високий ступінь захищеності.

FEK застосовується для створення ключів відновлення. Для цього FEK шифрується за допомогою одного або декількох відкритих ключів відновлення. Список FEK, зашифрованих для цілей відновлення, зберігається разом із зашифрованим файлом в спеціальному атрибуті EFS, званому полем відновлення даних (Data Recovery Field, DRF). Завдяки існуванню набору зашифрованих ключів FEK агенти відновлення даних можуть дешифрувати файл. Для шифрування ключа FEK в полі DRF необхідна тільки відкрита частина пари ключів відновлення, її присутність в системі необхідна у будь-який момент часу для нормального функціонування файлової системи. Сама процедура відновлення виконується досить рідко, коли користувач звільняється з організації або забуває приватну частину ключа. Тому агенти відновлення можуть зберігати приватну частину ключів відновлення в

безпечному місці, наприклад на смарт-картах або інших добре захищених пристроях.

EFS тісно взаємодіє з NTFS 5.0. Тимчасові файли, створювані додатками, успадковують атрибути оригінальних файлів (якщо файли знаходяться в розділі NTFS). Разом з файлом шифруються також і його тимчасові копії. EFS знаходиться в ядрі Windows і використовує для зберігання ключів спеціальний пул, що не вивантажується на жорсткий диск. Тому ключі ніколи не потрапляють у файл підкачки.

У Windows Server 2003 файлова система EFS має деякі нові можливості:

- із зашифрованими файлами можуть працювати декілька користувачів. Користувач, що зашифрував файл, може дозволити іншим локальним і доменним користувачам (на комп'ютерах під управлінням Windows 2000 і Windows XP) працювати з цим файлом;
- можна шифрувати автономні папки і файли (offline folders);
- агент відновлення (recovery agent) за умовчанням не використовується;
- стандартний алгоритм шифрування – Advanced Encryption Standard, AES (Rijndael) (256 біт). Алгоритм DESX, що використовується за умовчанням системою EFS в Windows 2000 і Windows XP Professional, не може застосовуватися для шифрування файлів в Windows Server 2003;
- замість AES може використовуватися алгоритм шифрування 3DES (128 або 168 біт), для цього потрібно змінити політику безпеки;
- зашифровані файли можуть розташовуватися у веб-папках;
- сертифікати EFS можуть автоматично доставлятися користувачу службами сертифікатів (Certificate Services) і механізмом автоматичного підпису сертифікатів;
- особисті ключі можуть зберігатися і відновлюватися за допомогою засобів архівації, що є в службах сертифікатів;
- вся службова інформація, що зберігається на диску, не просто видаляється, а очищується (заповнюється порожніми байтами); це збільшує захищеність шифрованих даних.

Конфігурація EFS, встановлювана за умовчанням, дозволяє користувачу шифрувати свої файли без жодного втручання з боку адміністратора. В цьому випадку EFS автоматично генерує для користувача пару ключів (відкритий і особистий), що застосовуються для криптозахисту даних, і підписує сертифікат.

Шифрування і дешифрування файлів може бути виконане як для певних файлів, так і для цілого каталогу. Ці операції прозорі для користувача. При

шифруванні каталогу автоматично шифруються і всі його файли і підкаталоги. Кожен файл має унікальний ключ, що дозволяє легко виконувати операцію перейменування. Якщо ви перейменовуєте файл, що знаходиться в зашифрованому каталозі, і переносите його в незашифрований каталог, сам файл залишається зашифрованим (за умови, що цільовий каталог знаходиться на томі NTFS 5.0). Засоби шифрування і дешифрування доступні через Windows Explorer. Крім того, можна використовувати всі можливості шифрування даних за допомогою набору утиліт командного рядка і інтерфейсів адміністрування.

Найсерйозніша і, на жаль, доволі поширена помилка при роботі з EFS полягає у тому, що користувачі шифрують дані на локальному комп'ютері, а потім встановлюють заново операційну систему. В цьому випадку **дані будуть безповоротно втрачені**, оскільки доступ до них мали тільки два користувачі тієї системи, в якій дані були зашифровані: користувач, що виконав цю операцію, і агент відновлення. Помилка полягає у тому, що для розшифрування даних необхідно пред'явити сертифікати одного з названих користувачів, а для цього відповідні сертифікати потрібно було експортувати і зберегти.

EFS має в своєму розпорядженні вбудовані засоби відновлення зашифрованих даних за умов, коли невідомий приватний ключ користувача. Користувачі, які можуть відновлювати зашифровані дані за умов втрати приватного ключа, називаються агентами відновлення даних<sup>1</sup>. Агенти відновлення даних мають сертифікат (X.509 v.3) на відновлення файлів і особистий ключ, за допомогою яких виконується операція відновлення зашифрованих файлів. Використовуючи ключ відновлення, можна одержати тільки генерований випадковим чином ключ, за допомогою якого був зашифрований конкретний файл. Тому агенту відновлення не може випадково стати доступною інша конфіденційна інформація.

---

<sup>1</sup> Політики відновлення в Windows XP/2003 працюють інакше, ніж в Windows 2000. За умовчанням на комп'ютерах під управлінням Windows Server 2003 агенти відновлення не створюються і політика відновлення не перешкоджає роботі EFS. Це означає, що відновити зашифровану інформацію можуть тільки ті користувачі, які її зашифрували.

## Завдання до виконання роботи

1. Створити на томі NTFS нову папку; у властивостях об'єкту перейти на вкладку "Безопасность" (рис. 19). (Звернути увагу на те, які дозволи призначені за замовчуванням.) Для того, щоб дозволити усім користувачам створювати файли і папки у цій папці, але заборонити її видаляти, а також для перегляду та редагування елементарних дозволів, натисніть кнопку "Дополнительно". Щоб додати елементарний дозвіл для користувача чи групи натисніть "Добавить" (рис. 20); додайте суб'єкта безпеки та задайте для нього дозволи (рис. 21). (Зверніть увагу на меню "Применять", яке управляє об'єктами безпеки, на які поширюватиметься заданий дозвіл!)

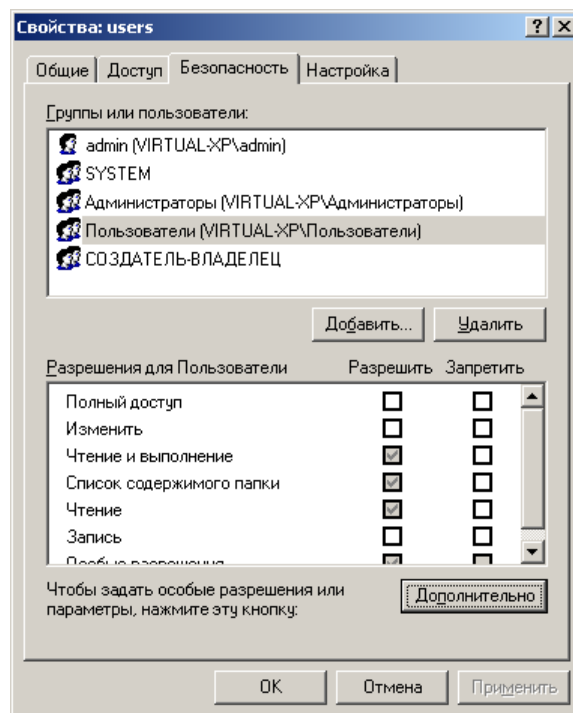


Рис. 19. Вкладка "Безпека" властивостей об'єкту файлової системи.

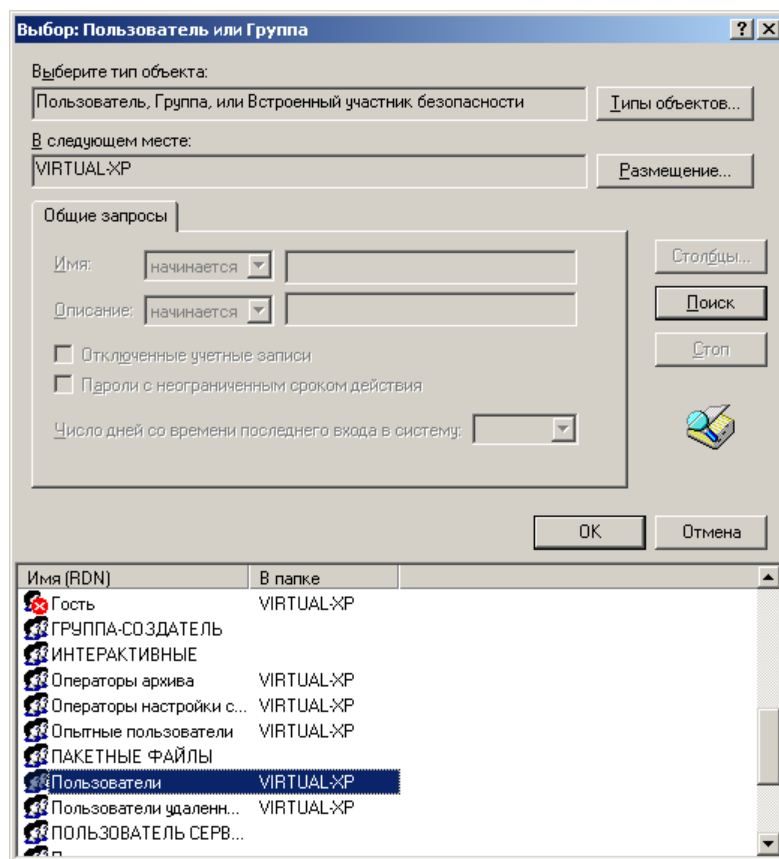


Рис. 20. Вибір суб'єкту безпеки.

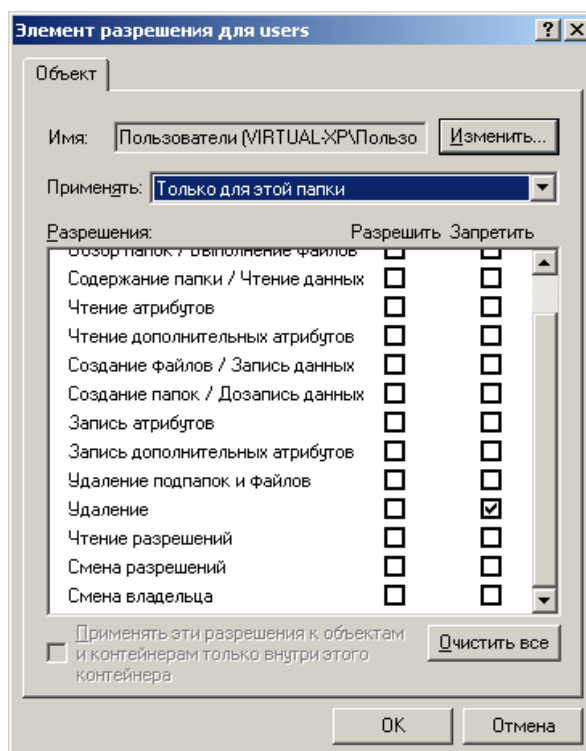


Рис. 21. Вікно спеціальних дозволів.

2. Увійти до системи під іншим користувачем (за необхідності створивши його) та переконатися у неможливості видаляти цю папку (рис. 22), однак маючи змогу створювати в ній файли та підпапки. Створити таку підпапку; переконатись, що як власник об'єкту цей користувач має право на зміну усіх дозволів. Заборонити групі "Адміністратори" повний доступ до створеної підпапки.

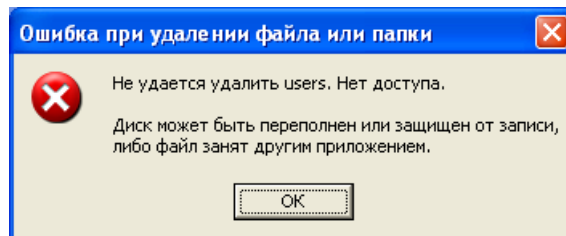


Рис. 22. Повідомлення системи про відмову в доступі на виконання операції.

3. Увійти до системи як користувач з адміністративними повноваженнями. Переконатись у відсутності доступу до підпапки, створеної у ході виконання п. 2 лабораторної роботи. Зайти на вкладку "Безопасность" властивостей об'єкту. У звіті до лабораторної роботи пояснити отримане повідомлення (рис. 23). В додаткових параметрах безпеки змінити власника папки (див рис. 17). Звернути увагу на можливість зміни власника як тільки для поточного об'єкту, так і для субконтейнерів і об'єктів. Переглянути список управління доступом після зміни власника – які суб'єкти та які права доступу є в цьому списку?

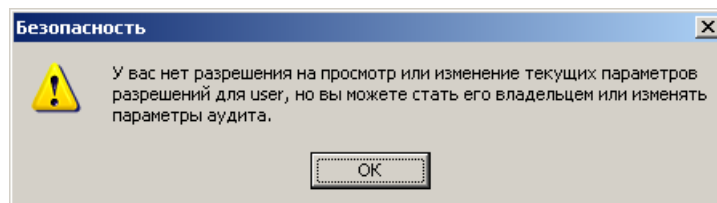


Рис. 23. Повідомлення системи безпеки.

4. Для приведення налаштування безпеки усіх вкладених субконтейнерів і об'єктів до шаблонного зразка батьківської папки використати відмітку "Заменить разрешения для всех дочерних объектов..." вкладки "Разрешения" додаткових параметрів безпеки для папки (рис. 24).



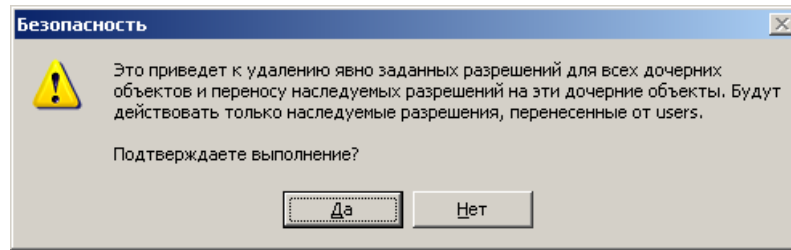


Рис. 24. Повідомлення системи безпеки при заміні дозволів для усіх дочірніх об'єктів.

5. Користувачем з адміністративними правами перейти на вкладку "Квота" (рис. 25) властивостей NTFS тому (за необхідності конвертувати існуючий FAT том, або створити новий). Включити управління квотами у "м'якому" режимі. У вікні "Записи квот" (рис. 26) скориставшись меню "Квота" створити індивідуальний запис квоти для певного користувача (рис. 27).

Увійти до системи під іншим користувачем. Записати на том з квотами файли сумарним обсягом більшим від порогу попереджень, але меншим за розмір квоти.

Увійти до системи під третім користувачем. Записати на том з квотами файли сумарним обсягом більшим за розмір квоти.

Користувачем з адміністративними правами переглянути записи квот для цього тому (рис. 28). Включити квоти у "жорсткому" режимі (для цього поставити відмітку "Не выделять место на диске при превышении квоты").

Увійти до системи під іншим користувачем. Спробувати записати на том з квотами файли сумарним обсягом більшим за розмір квоти. Переконатись у неможливості такої операції (рис. 29).

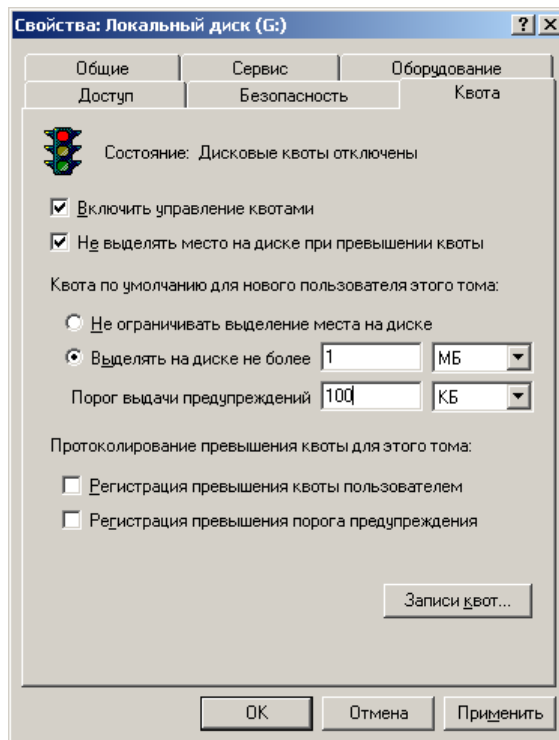


Рис. 25. Вкладка квот у властивостях дискового тому.

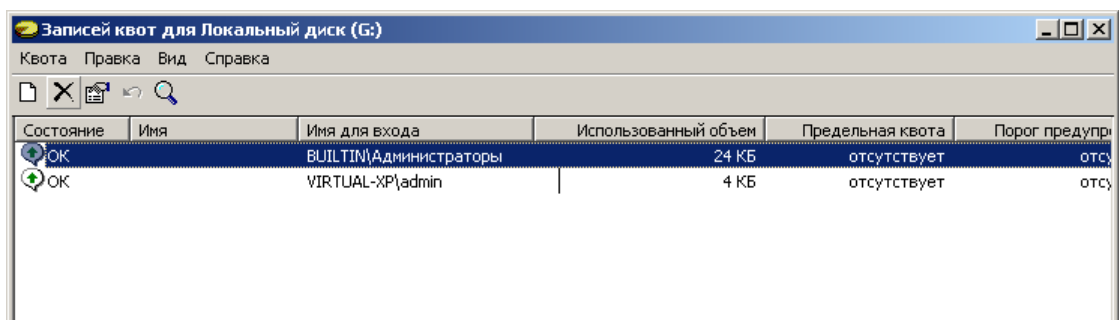


Рис. 26. Вікно записів квот для дискового тому.

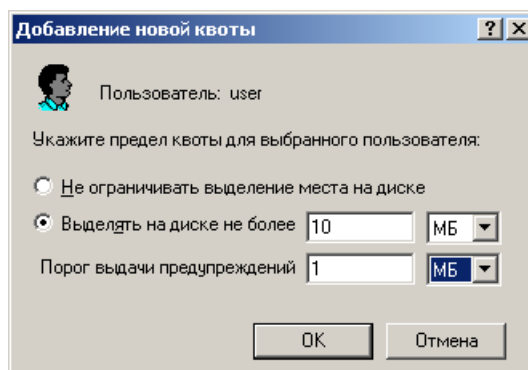


Рис. 27. Додавання нового запису квоти.

Состояние	Имя	Имя для входа	Использованный объем	Предельная квота	Порог предупреждений
Превышен предел	Новий користувач	VIRTUAL-XP\new user	8,18 МБ	1 МБ	100 КБ
Предупреждение	user	VIRTUAL-XP\user	7,39 МБ	10 МБ	1 МБ
OK		BUILTIN\Администраторы	24 КБ	отсутствует	отсутствует
OK		VIRTUAL-XP\admin	4 КБ	отсутствует	отсутствует

Рис. 28. Вікно записів квот для дискового тому (один користувач перевищив поріг квоти, а один – поріг попереджень).

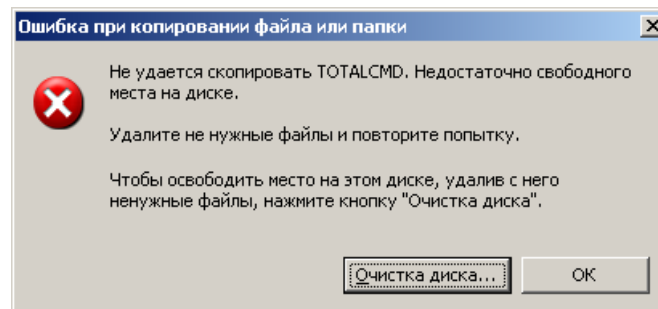


Рис. 29. Повідомлення системи при спробі записати файли понад квоту.

6. Створити агента відновлення шифрованих даних. Для цього виконати наступні кроки:

I. Створення сертифікату агента відновлення:

- Увійти в систему як адміністратор.
- У вікні консолі ввести команду `cipher /R:Ім'яФайлу` – без розширення (рис. 30).
- Ввести і підтвердити пароль, о захищає приватний ключ.

В поточному каталозі будуть створені два файли: з розширенням `seg` (містить тільки згенерований ключ) і з розширенням `prfx` (містить і ключ, і сертифікат агента відновлення).

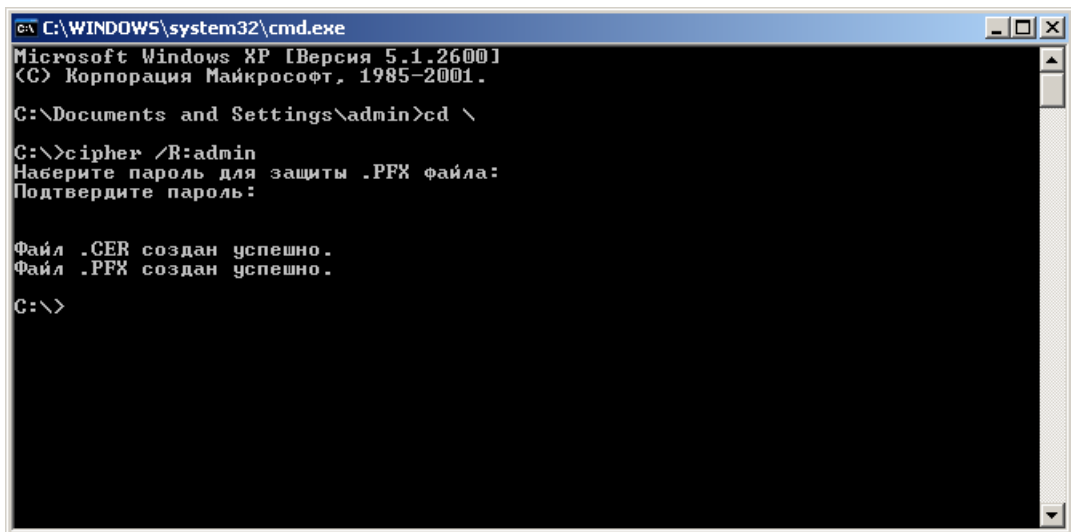


Рис. 30. Створення сертифікату агента відновлення.

II. Імпорт сертифікату, за допомогою якого можна відновлювати індивідуальні файли користувачів:

- Відкрийте оснастку **Сертификаты**, вузол **Личные** (рис. 31).
- Імпортуйте створений **PFX**-файл (зверніть увагу на розширення сертифікату!).

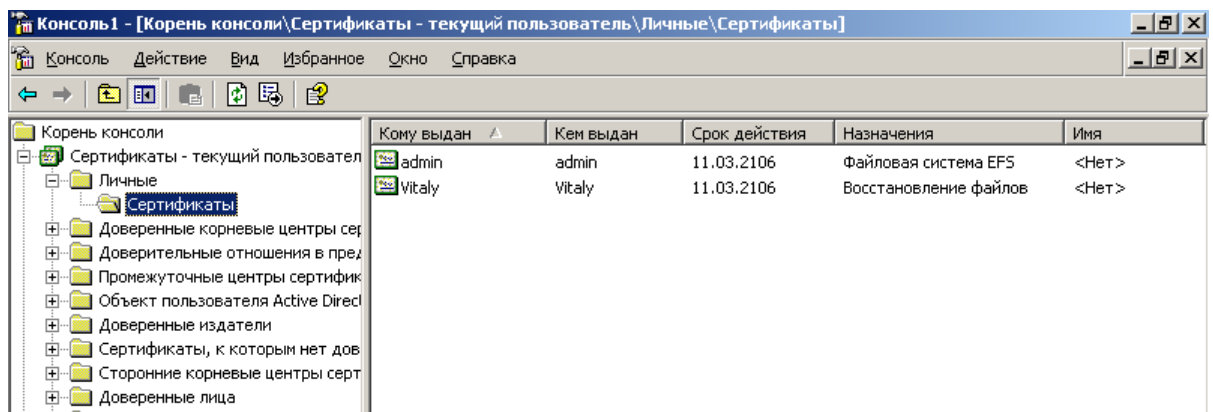


Рис. 31. Імпорт сертифікату агента відновлення.

III. Призначення політики агента відновлення для операцій шифрування:

- Запустіть оснастку **Редактор объекта групповой политики**.
- Виберіть вузол **Политики открытого ключа | Файловая система EFS** (рис. 32).
- В контекстному меню виконайте команду **Добавить агент восстановления данных**.
- У вікні майстра **Мастер добавления агента восстановления** натисніть кнопку **Обзор папок** і вкажіть шлях до створеного раніше файлу з розширенням cer.

- Завершіть роботу майстра натиснувши кнопки **Далее** та, на наступній сторінці, **Готово**.

Сертифікат буде імпортовано, а його власник стане агентом відновлення шифрованих даних на цьому комп'ютері. (Зверніть увагу, що в стовпчику **Назначения** імпортованого сертифікату вказано **Восстановление файлов**).

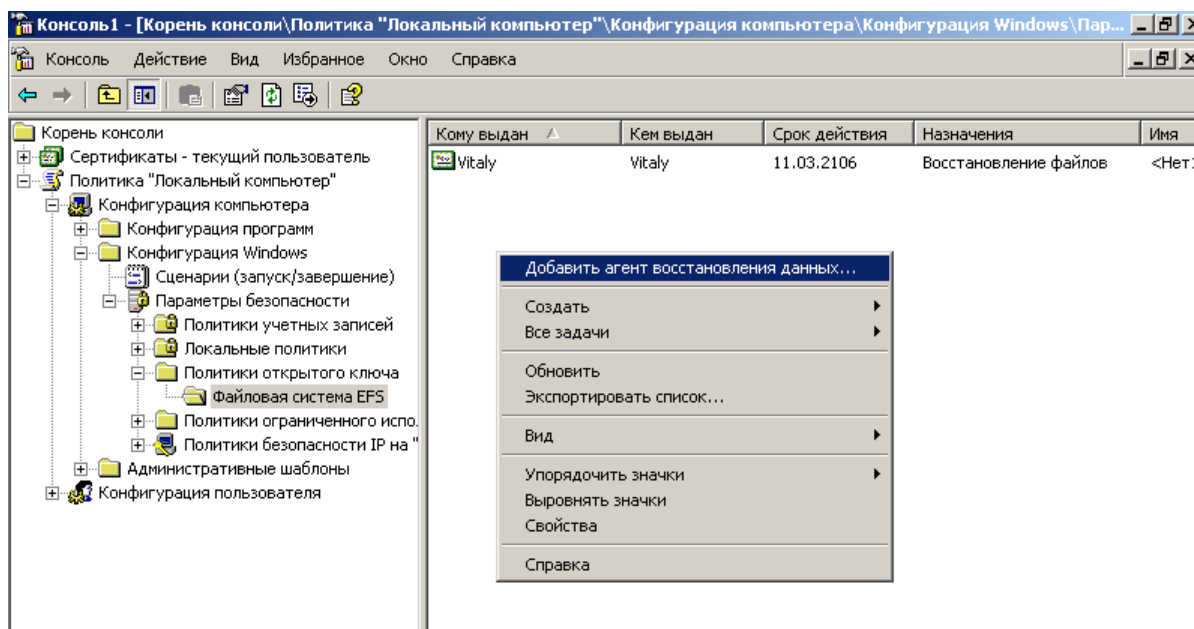


Рис. 32. Створення політики агента відновлення шифрованих даних.

7. Увійшовши до системи під декількома користувачами зашифруйте по одному файлу для кожного користувача. Для цього у властивостях файлу (вкладка "Общие") натисніть кнопку "Дополнительно" і поставте відмітку "Шифровать содержимое для защиты данных" (рис. 33). Переконайтесь, що кожен користувач може розшифрувати тільки свої файли, а після шифрування першого файлу створюється сертифікат з призначенням **Файловая система EFS** (перевірити за допомогою оснастки **Сертификаты**).

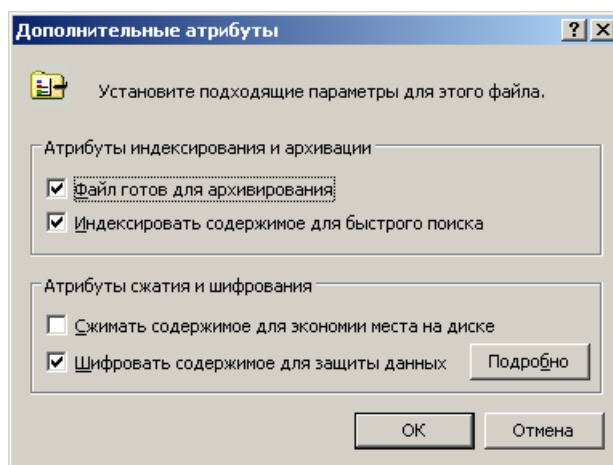


Рис. 33. Вікно встановлення додаткових атрибутів файлу.

При потребі спільного доступу декількох користувачів до одного шифрованого файлу у вікні додаткових атрибутів файлу оберіть кнопку "Подробно" (рис. 34). Після цього у вікні "Пользователи, которым разрешен доступ к файлу" можна додати користувачів, яким дозволено розшифровувати цей файл (основною умовою є наявність в системі сертифікатів цих користувачів). Крім того, зверніть увагу, що після призначення політики агента відновлення шифрованих даних у вікні деталей щодо шифрування кожного файлу міститься ім'я агента відновлення (рис. 34). Переконайтесь, що користувачі, яким дозволили спільний доступ, можуть читати (тобто розшифровувати) цей файл, в той як інші – ні.

(Якщо треба надати певному користувачу доступ до ВСІХ шифрованих файлів іншого користувача, можна експортувати сертифікат користувача, що надає свої файли – але обов'язково у rfx форматі – і імпортувати цей файл іншому користувачу для надання доступу.)

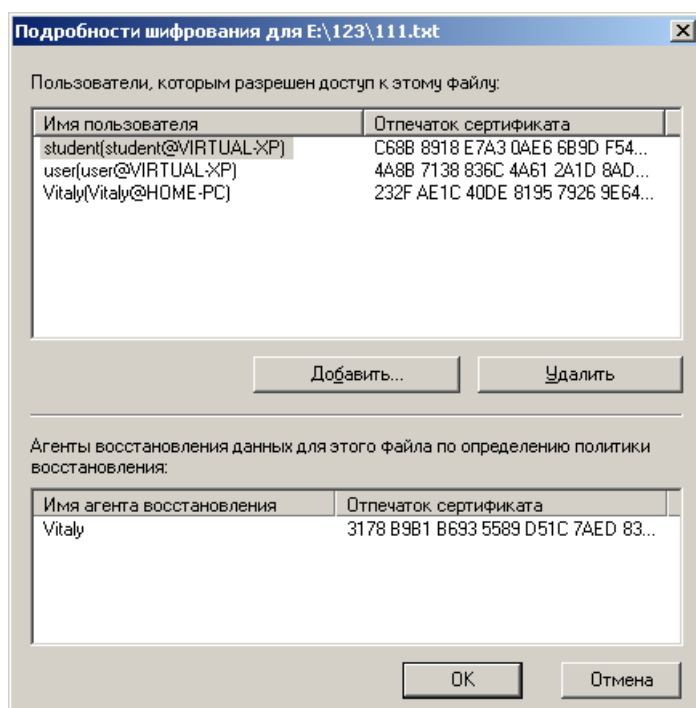


Рис. 34. Налаштування шифрованого файлу на спільний доступ декількох користувачів при діючій політиці агента відновлення.

У звіті до лабораторних робіт описати та пояснити отримані результати.

### **Контрольні запитання.**

1. Чим відрізняються дозволи "Изменить" та "Запись"?
2. Чи можна заборонити доступ до об'єктів файлової системи адміністратору комп'ютера?
3. Хто може брати об'єкти у власність?
4. Об'єкт файлової системи може брати у власність група "Администраторы". Яке призначення такої можливості?
5. Чи можна призначити індивідуальний розмір квот для кожного користувача, групи?
6. Призначення файлової системи EFS.
7. Хто може розшифрувати файл, зашифрований іншим користувачем?

## СПИСОК ЛИТЕРАТУРЫ

1. **Microsoft Corporation** Microsoft Windows XP Professional. Учебный курс MCSA/MCSE. – М.: Издательско-торговый дом "Русская Редакция", 2003. – 1008 стр.
2. **Microsoft Corporation** Microsoft Windows 2000 Active Directory Services. Учебный курс MCSE. – М.: Издательско-торговый дом «Русская редакция», 2004. – 608 с.
3. **Руссинович М., Соломон Д.** Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP и Windows 2000. – М.: Издательско-торговый дом «Русская редакция»; СПб.: Питер, 2005. – 992 с.
4. **Вишневский А.** Windows Server 2003. Для профессионалов. – СПб.: Питер, 2004. – 767 с.
5. **К. Айвенс** Microsoft Windows Server 2003. Полное руководство. – М.: Издательство "СП ЭКОМ", 2004.– 896 с.



НАВЧАЛЬНЕ ВИДАННЯ

**УПРАВЛІННЯ КОРИСТУВАЧАМИ І ГРУПАМИ, СПІЛЬНИЙ ДОСТУП  
ДО ОБ'ЄКТІВ ФАЙЛОВОЇ СИСТЕМИ У WINDOWS XP**

**МЕТОДИЧНІ ВКАЗІВКИ**

до виконання лабораторних робіт  
з дисципліни „Адміністрування та безпека комп'ютерів”  
для студентів спеціальності  
„Програмне забезпечення автоматизованих систем”

*Укладачі*

Яковина Віталій Степанович  
Білас Орест Євгенович

*Редактор*

*Комп'ютерне верстання*