ЛАБОРАТОРНА РОБОТА №7

ВИКОРИСТАННЯ ГРУПОВИХ ПОЛІТИК І ШАБЛОНІВ БЕЗПЕКИ В МЕРЕЖІ З ДОМЕННОЮ СТРУКТУРОЮ НА БАЗІ СІМЕЙСТВА ОС WINDOWS

Тема: Організаційні підрозділи. Групові політики. Права доступу. Аудит доступу до ресурсів.

Мета: Застосування групових політик

ЗАВДАННЯ

1. Створити ієрархію організаційних підрозділів. (*Створити підрозділ ОР1. В ньому ОР11 та ОР12 і додати користувачів у дані підрозділи.*).
2. На верхньому рівні ор1 застосувати групову політику. перевірити виконання групової політики. (*Прибрати з меню «Пуск» пункт «Виконати»*).
3. На рівні ОР11 провести блокування виконання групової політики верхнього рівня підрозділа ОР1. перевірити виконання групової політики.
4. На рівні ОР1 заборонити блоківання групових політик на нижніх рівнях. перевірити виконання.
5. Створити групову політику на рівні підрозділу ОР11. Перевірити виконання групової політики. (*Прибрати з меню «Пуск» пункт «Знайти»*).

Перелік додаткових завдань для самостійного опрацювання:

1. Створити групу користувачів. додати користувачів до неї.

2. Розмежувати доступ до об`єктів домену для груп користувачів, використовуючи дозволи NTFS.
3. Ознайомитись з властивостями профілів користувачів в доменній структурі. *(Налаштування профіля з переміщенням)*

ТЕОРЕТИЧНИЙ МАТЕРІАЛ

Частина 1 Організаційні підрозділи (Organizational Units)

Керування Організаційними підрозділами, делегування повноважень

Призначення Організаційних підрозділів (ОП, Organizational Units, OU) - організація ієрархічної структури об'єктів AD у середині домену. Як правило, ієрархія ОП у домені відбиває організаційну структуру компанії.

На практиці використання ОП (крім ієрархічної організації об'єктів) зводиться до двох завдань:

- делегування адміністративних повноважень на керування об'єктами ОП якому-небудь користувачеві або групі користувачів;
- застосування групових політик до об'єктів, що входять в ОП.

Делегування адміністративних повноважень на керування об'єктами ОП якому-небудь користувачеві або групі дозволяє в більших організаціях розподілити навантаження по адмініструванню облікових записів між різними співробітниками, не збільшуючи при цьому кількість користувачів, що мають адміністративні права на рівні всього домену.

Розглянемо на прикладі процедуру надання якому-небудь користувачеві адміністративних прав на керування ОП:

- Відкриємо консоль "Active Directory Users and Computers". □ Створимо в домені підрозділ, скажімо, з іменем OU-117 (Рис.3.1,3.2).

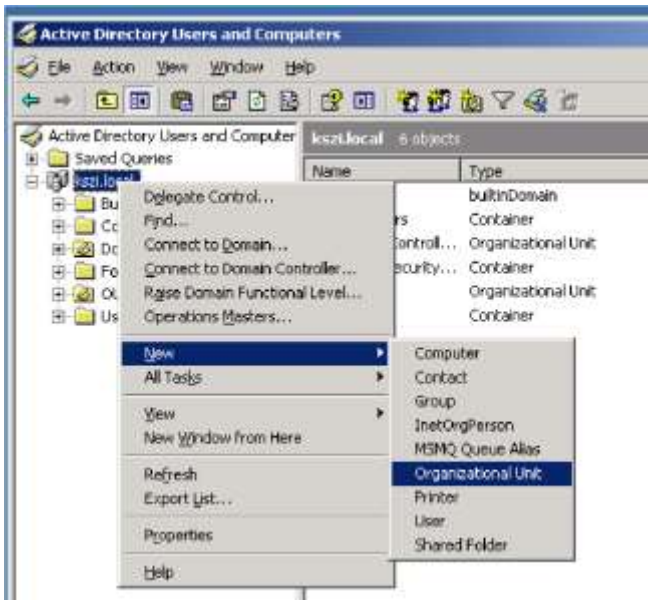

Рис.3.1

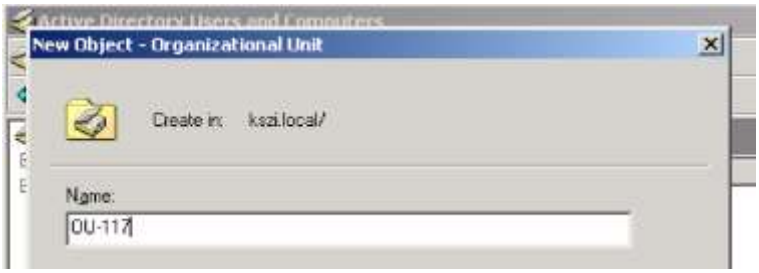

Рис.3.2

- Перемістимо в цей ОП декілька наявних у домені облікових записів (або створимо нові).
- Клацнемо правою кнопкою миші на підрозділі OU-117 і виберемо пункт меню "Delegate Control…". Запуститься "Delegation of Control Wizard"(Рис.3.3).

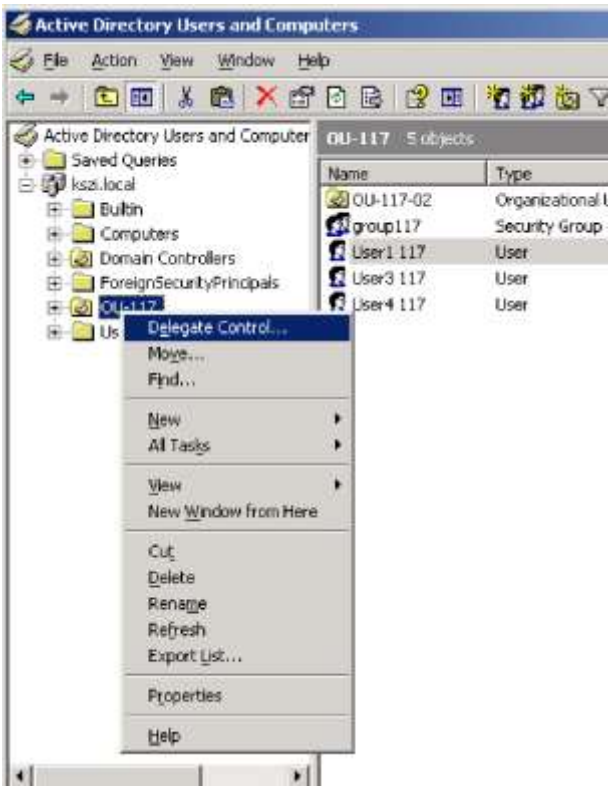

Рис.3.3

 Виберемо користувача (або групу), якому будемо делегувати керування даним ОП. Нехай це буде користувач User1. Натиснемо "Next". (Рис.3.4).

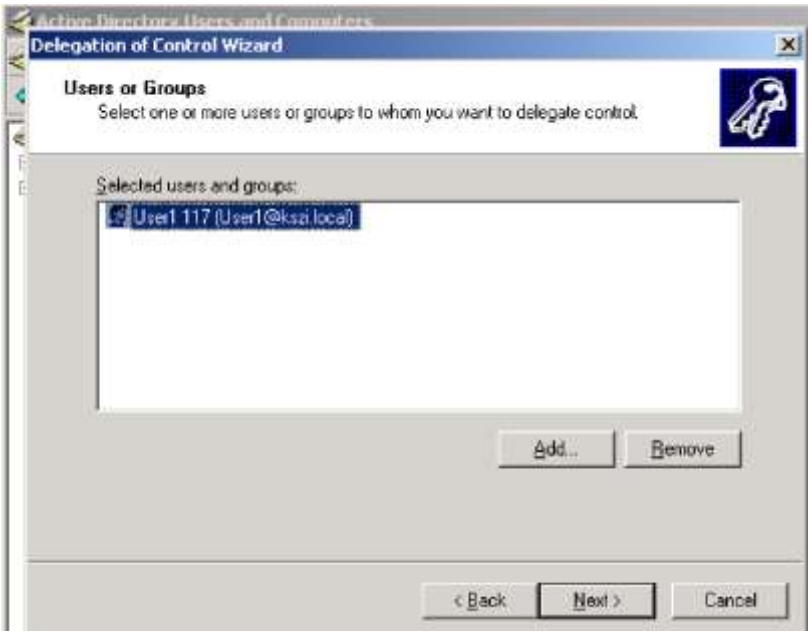

Рис.3.4

 Виберемо набір адміністративних завдань, які делегуються даному користувачеві (Рис.3.5).

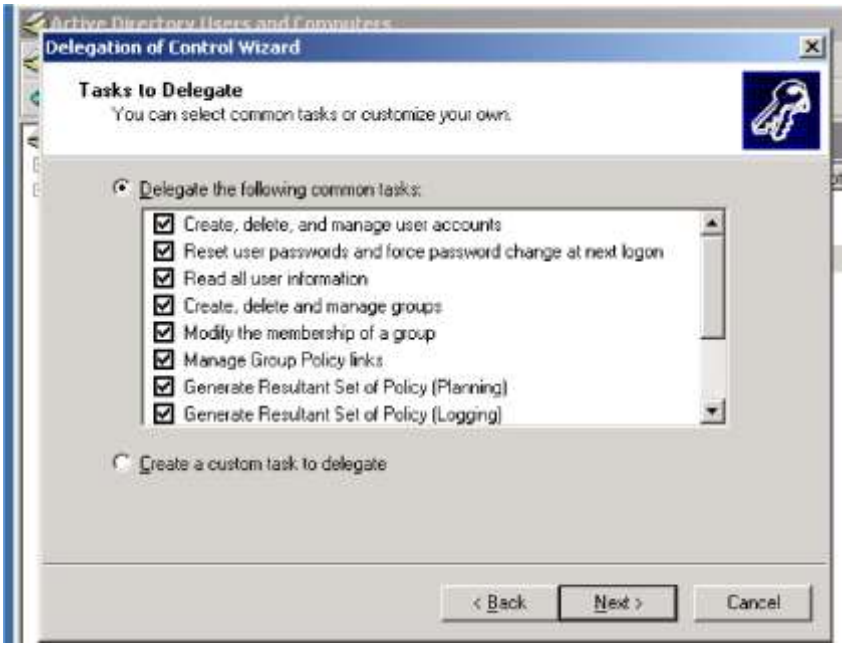

Рис.3.5

 По завершенню майстра - натиснемо кнопку "Finish" (Рис.3.6).

Рис.3.6

Якщо тепер увійти в систему на контролері домену з обліковим записом User1 (за умови, що в користувача User1 є права локального входу в систему на контролері домену), запустити консоль "Active Directory Users and Computers", то користувач User1 зможе виконувати будь-які операції з об'єктами організаційного підрозділу OU-117

Групові політики

Групові політики: призначення, склад, стандартні політики домену, порядок застосування політик (локальні, сайт, домен, ОП), застосування політик і права доступу, спадкування й блокування застосування.

Керування робочими станціями, серверами, користувачами у великій організації - дуже трудомістке завдання. Механізм Групових політик (Group Policy) дозволяє автоматизувати даний процес керування. За допомогою групових політик (ГП) можна настроювати різні параметри комп'ютерів і користувацького робочого середовища відразу в масштабах сайту AD, домену, організаційного підрозділу (деталізацію настроювань можна проводити аж до окремого комп'ютера або користувача). Настроювати можна широкий набір параметрів - сценарії входу в систему й завершення сеансу роботи в системі, параметри Робочого стола й Панелі керування, розміщення особистих папок користувача, настроювання безпеки системи (політики паролів, керування обліковими записами, аудита доступу до мережних ресурсів, керування сертифікатами і т.д.), розгортання додатків і керування їх життєвим циклом.

Кожний об'єкт групових політик (GPO, Group Policy Object) складається із двох частин:

- контейнера групових політик (GPC, Group Policy Container), що зберігається в БД Active Directory;
- шаблону групових політик (GPT, Group Policy Template) контролера, що зберігається у файловій системі, домену, у підпапках папки SYSVOL. Місце, у якому зберігаються шаблони політик, - це папка %systemroot%\SYSVOL\sysvol\

< ім'я домену>\Policies, і ім'я папки шаблону збігається з глобальним унікальним ідентифікатором (GUID) об'єкта Групова політика.

Кожний об'єкт політики містить два розділи:

- конфігурація комп'ютера;
- конфігурація користувача. (Рис.3.7).

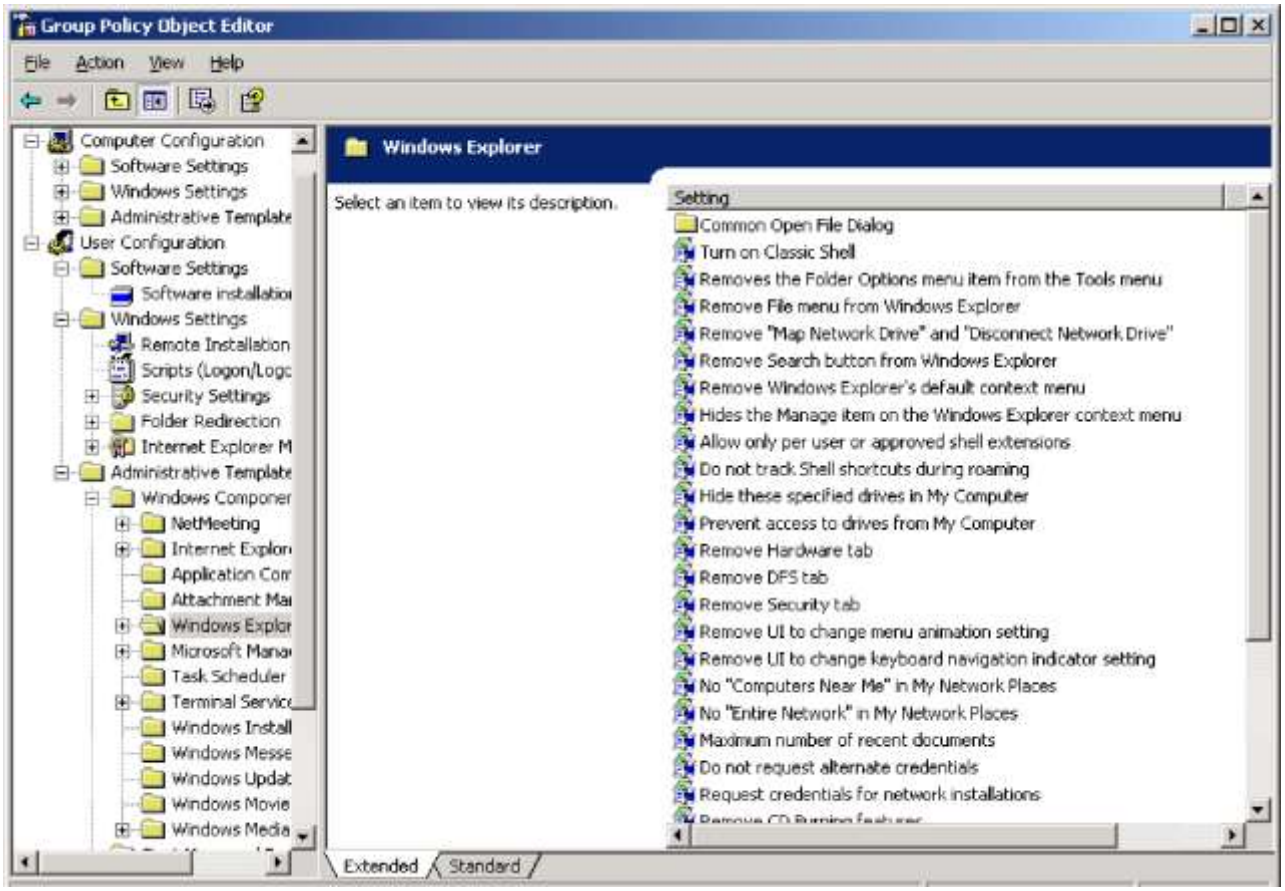

Рис.3.7

Параметри цих розділів застосовуються відповідно або до настроювань комп'ютера, або до настроювань середовища користувача.

Кожний об'єкт політики може бути прив'язаний до того або іншого об'єкту AD - сайту, домену або організаційного підрозділу (а також до декількох об'єктів одночасно).

Задання параметрів групових політик проводиться Редактором групових політик, який можна відкрити в консолі керування відповідним об'єктом AD (Рис.3.8).

Рис.3.8

На Рис.3.8 показана закладка "Group Policy" властивостей домену kszi.local. На даній закладці можна виконати наступні дії:

- кнопка "New" - створити новий об'єкт ГП;
- кнопка "Add" - прив'язати до даного об'єкта AD існуючий об'єкт ГП;
- кнопка "Edit" - відкрити редактор групових політик для обраного об'єкта ГП;
- кнопка "Options…" - заборонити перекривання (поле "No override") параметрів даної об'єкта ГП іншими політиками або блокування на більш низькому рівні ієрархії AD або відключити (поле "Disabled") даний об'єкт ГП;
- кнопка "Delete…" - видалити обраний об'єкт ГП або видалити прив'язку об'єкта ГП до даного рівня AD;
- кнопка "Properties" - відключити комп'ютерний або користувацький розділи політики або настроїти дозвіл на використання даного об'єкта ГП;
- поле "Block Policy inheritance" - заборонити застосування політик, прив'язаних до більш високих рівнів ієрархії AD;
- кнопки "Up" і "Down" - керування порядком застосування політик на даному рівні AD (політики, розташовані в списку вище, мають більш високий пріоритет).

При завантаженні комп'ютера й аутентифікації в домені до нього застосовуються комп'ютерні розділи всіх прив'язаних політик. При вході користувача в систему до користувача застосовується користувацький розділ усіх групових політик. Політики, прив'язані до деякого рівня ієрархії об'єктів AD (сайту, домену, підрозділу) успадковуються всіма об'єктами AD, що перебувають на більш низьких рівнях.

Порядок застосування політик:

- локальна політика;
- політики сайту Active Directory;
- політики домену;
- політики організаційних підрозділів.

Якщо в процесі застосування політик які-небудь параметри визначаються в різних політиках, то діючими значеннями параметрів будуть значення, назначені пізніше.

Є наступні методи керування застосуванням групових політик:

- блокування спадкування політик на будь-якому рівні ієрархії AD;
- заборона блокування конкретного об'єкта групових політик;
- керування пріоритетом застосування політик на конкретному рівні AD (кнопками "Вгору" і "Вниз");
- дозвіл на застосування політик (щоб політики якого-небудь об'єкта ГП застосовувалися до користувача або комп'ютера, даний користувач або комп'ютер повинен мати дозволи на цей об'єкт ГП "Read" і "Apply Group Policy").

Крім застосування політик у момент завантаження комп'ютера або входу користувача в систему, кожний комп'ютер постійно запитує оновлені політики на контролерах домену, завантажує їх і застосовує оновлені параметри (і до користувача, і до комп'ютера). Робочі станції домену та прості сервери запитують відновлення кожні 90 ± 30 хвилин, контролери домену обновляють свої політики кожні 5 хвилин. Обновити набір політик на комп'ютері можна примусово з командного рядка командою gpupdate (на комп'ютерах із системами Windows XP/2003).

Керування додатками

Розглянемо докладніше використання групових політик для розгортання додатків у мережах під керуванням Active Directory.

Групові політики можуть використовуватися для установки прикладних програм у масштабах усього домену або окремого організаційного підрозділу.

Використовуються наступні способи керування установкою додатків:

- призначення додатків комп'ютерам (при даному способі додаток, призначений комп'ютеру, автоматично встановлюється при завантаженні комп'ютера);
- призначення додатків користувачам (додаток установлюється при першому виклику даного додатка - при відкритті ярличка додатка або файлу, відповідного до даного додатка);
- публікація додатків користувачам (назва додатка додається до списку доступних для установки програм у вікні "Установка й видалення програм" у Панелі керування).

За допомогою політик можна управляти установкою додатків, які встановлюються за допомогою компонента Windows Installer, тобто для них пакет встановлення повинен бути створений у форматі файлу з розширенням ".msi". Якщо додаток можна встановити тільки за допомогою програми встановлення типу setup.exe або install.exe, то такі додатки можуть бути

опубліковані (але не призначені) після створення файлу типу ".zap", у якім задані відповідні параметри, необхідні для публікації засобами ГП.

Процес призначення додатків

Призначення пакета Group Policy Management Console ("Консоль керування груповими політиками") усім комп'ютерам домена kszi.local.

- Відкриємо закладку "Group Policy" властивостей домена. Створимо новий об'єкт ГП із іменем "GPMC"(Рис.3.9).

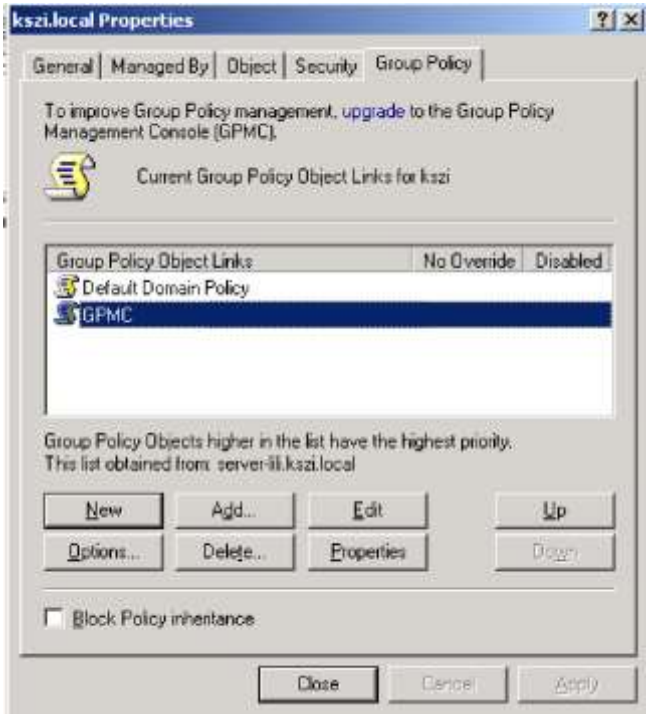

Рис.3.9

- Відкриємо редактор політик для політики GPMC, відкриємо "Computer Configuration", "Software Settings", на параметрі "Software installation" клацнемо правою кнопкою миші й виберемо "New - Package…"(Рис.3.10).

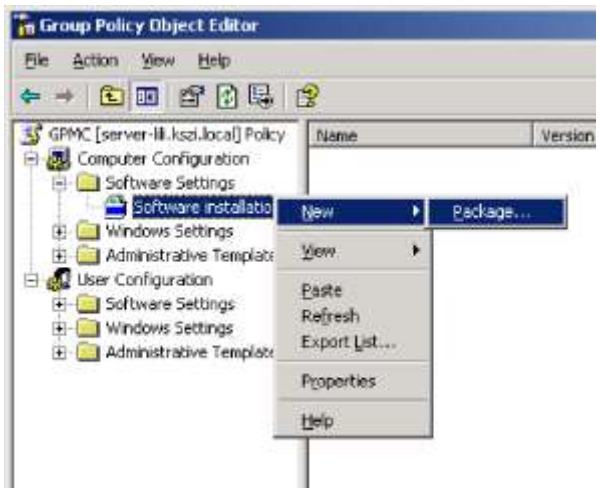

Рис.3.10

 Укажемо шлях до пакету "…\gpmc.msi". Виберемо метод розгортання "Assigned"(Рис.3.11).

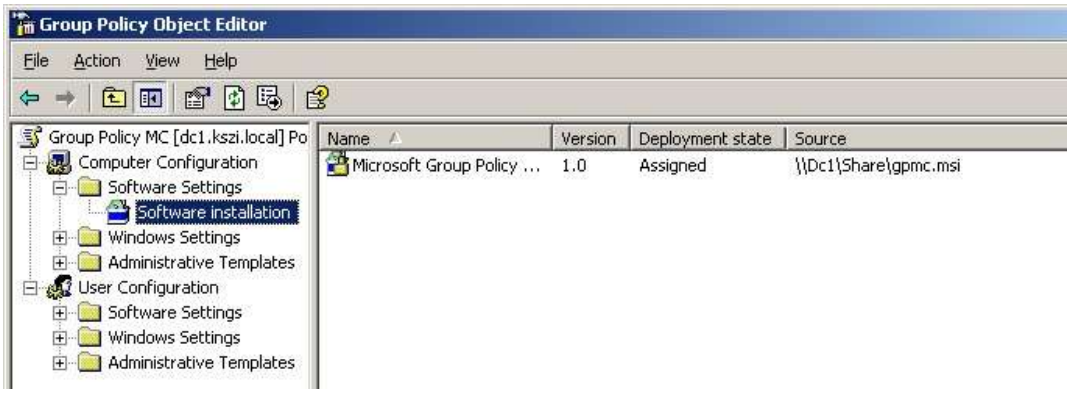

Рис.3.11

При завантаженні комп'ютера в домені в процесі застосування політик буде встановлений даний програмний пакет.

Процес публікації додатків

Публікація пакета Microsoft Office 2003 усім користувачам домену kszi.local.

- Відкриємо закладку "Group Policy" властивостей домену. Створимо новий об'єкт ГП із іменем "MS Office 2003".
- Відкриємо редактор політик для політики MS Office 2003, відкриємо "User Configuration", "Software Settings", на параметрі "Software Installation" клацнемо правою кнопкою миші й виберемо "New - Package…"(Рис.3.12).

Рис.3.12

- Укажемо мережний шлях до пакета "\\server\soft\…\Office 2003\PRO11.msi". Виберемо метод розгортання "Published", натиснемо "ОК"

Після застосування політик відкриємо Панель керування, виберемо "Установка й видалення програм", натиснемо кнопку "Установка програм", у вікні доступних для установки програм з'явиться назва пакета "Microsoft Office 2003"(Рис..3.13).

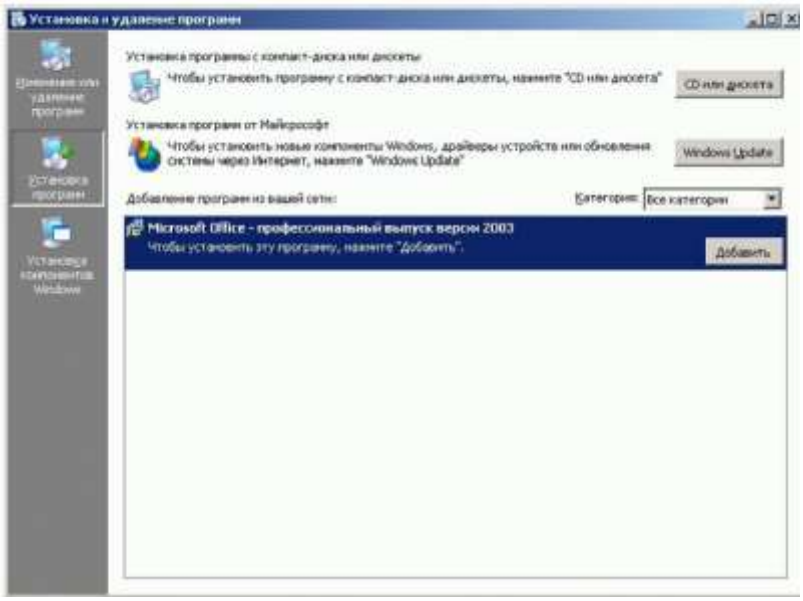

Рис..3.13

Group Policy Management Console

Як приклад установки пакета за допомогою призначення ми вибрали пакет MS Group Policy Management Console (Консоль керування груповими політиками). Комплект встановлення можна знайти в Центрі завантаження сайту корпорації Microsoft (пакет поширюється безкоштовно).

Розглянемо тепер докладніше, як працює цей пакет.

По-перше, установити його можна на комп'ютер із системами Windows XP/2003. При цьому управляти політиками пакет може й у доменах під керуванням Windows 2000.

По-друге, при перегляді властивостей якого-небудь домену або ОП закладка "Групові політики" після установки GPMC виглядає по-іншому(Рис.3.14):

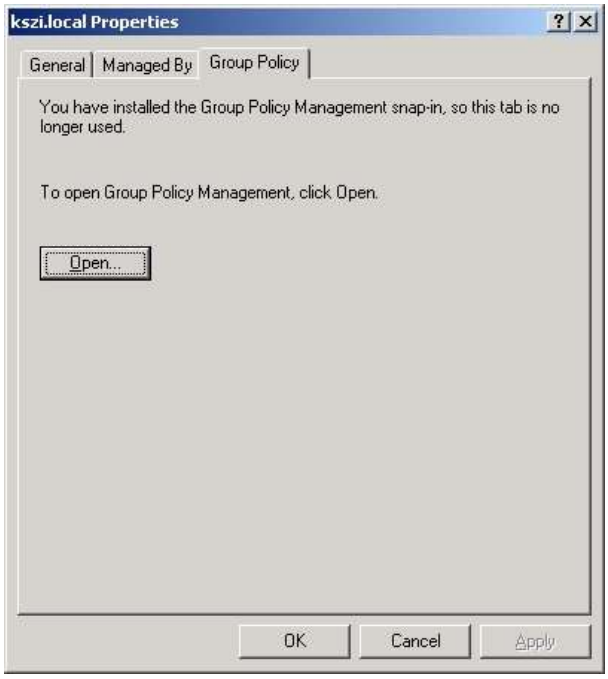

Рис.3.14

На цій закладці замість списку політик і безлічі кнопок тепер усього одна кнопка "Open…" ("Відкрити").

Відзначимо основні переваги цієї консолі в порівнянні з базовими можливостями системи.

- Наочне відображення ієрархії усередині домену з усіма об'єктами ГП, прив'язаними до різних рівнів ієрархії ОП (Рис.3.15):

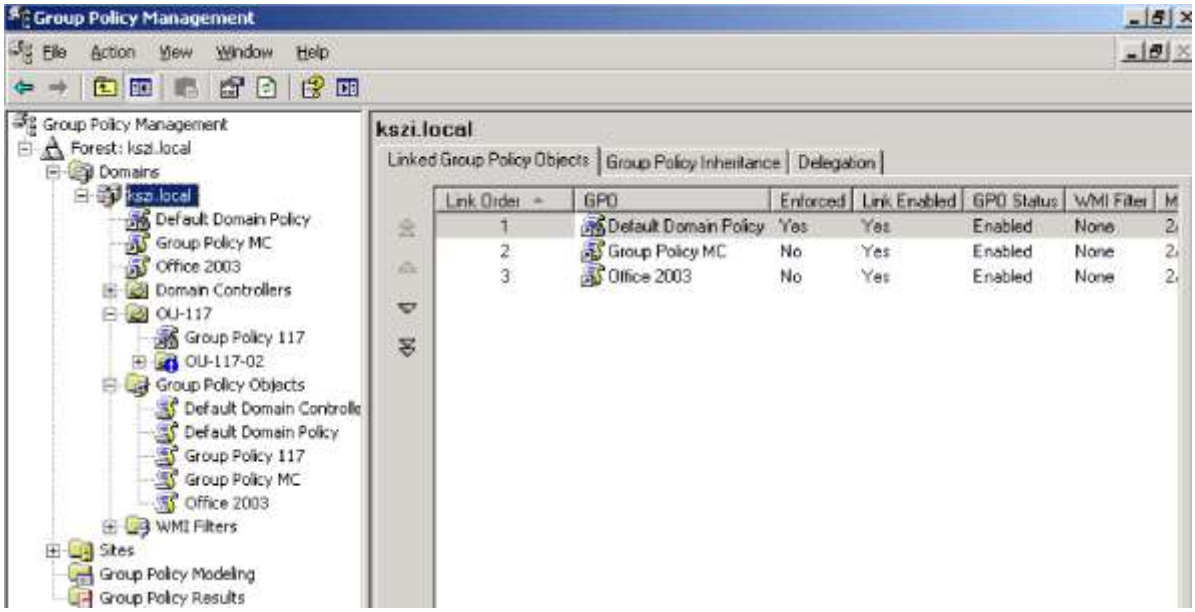

Рис.3.15

На малюнку добре видно всю ієрархію підрозділів усередині домену. Причому на кожному рівні відображається список політик, прив'язаних до даного рівня.

Наприклад, на рівні домену прив'язані політики: стандартна політика домену, політика Group Policy MC (призначення пакета GPMC) і політика Office 2003 (публікація пакета MS Office).

На рівні підрозділу OU-117 включене блокування спадкування політик (синій значок зі знаком оклику). Стандартна політика домену Default Domain Policy має властивість "Не перекривати" (невеликий значок праворуч від стрілки на піктограмі об'єкта ГП).

Включення параметра "Не перекривати" у цій консолі робиться так: клацнути правою кнопкою миші на об'єкті ГП і в контекстному меню вибрати пункт "Enforce".

У контейнері "Group Policy Objects" наведений повний список усіх об'єктів ГП.

Для виклику редактора політик потрібно клацнути правою кнопкою миші на об'єкті ГП і в контекстному меню вибрати пункт "Edit".

У розділі "Group Policy Modeling" можна визначити, який набір політики буде застосовуватися на тому або іншому рівні ієрархії AD (на Рис.3.16 виведений список політик, застосованих до підрозділу OU-117):

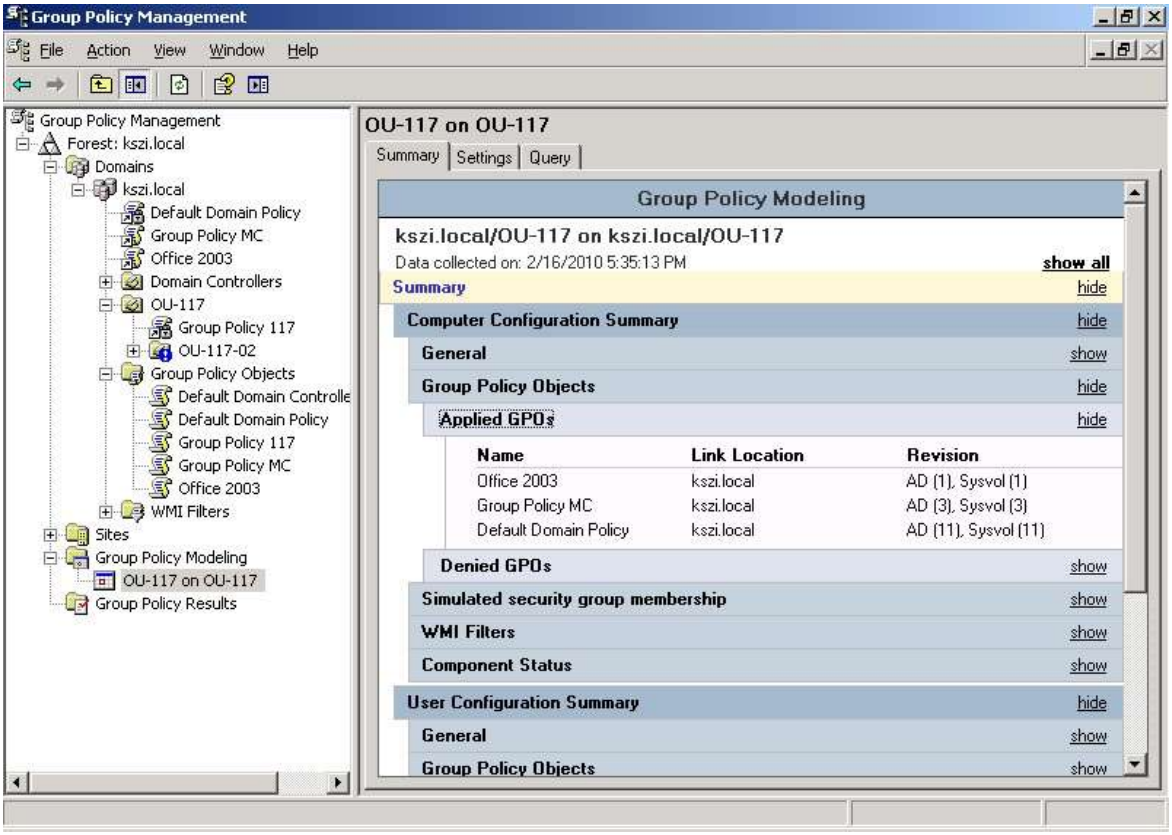

Рис.3.16

У розділі "Group Policy Results" можна визначити набір параметрів, застосованих до певного користувача або комп'ютера в результаті накладення всіх політик(Рис.3.17):

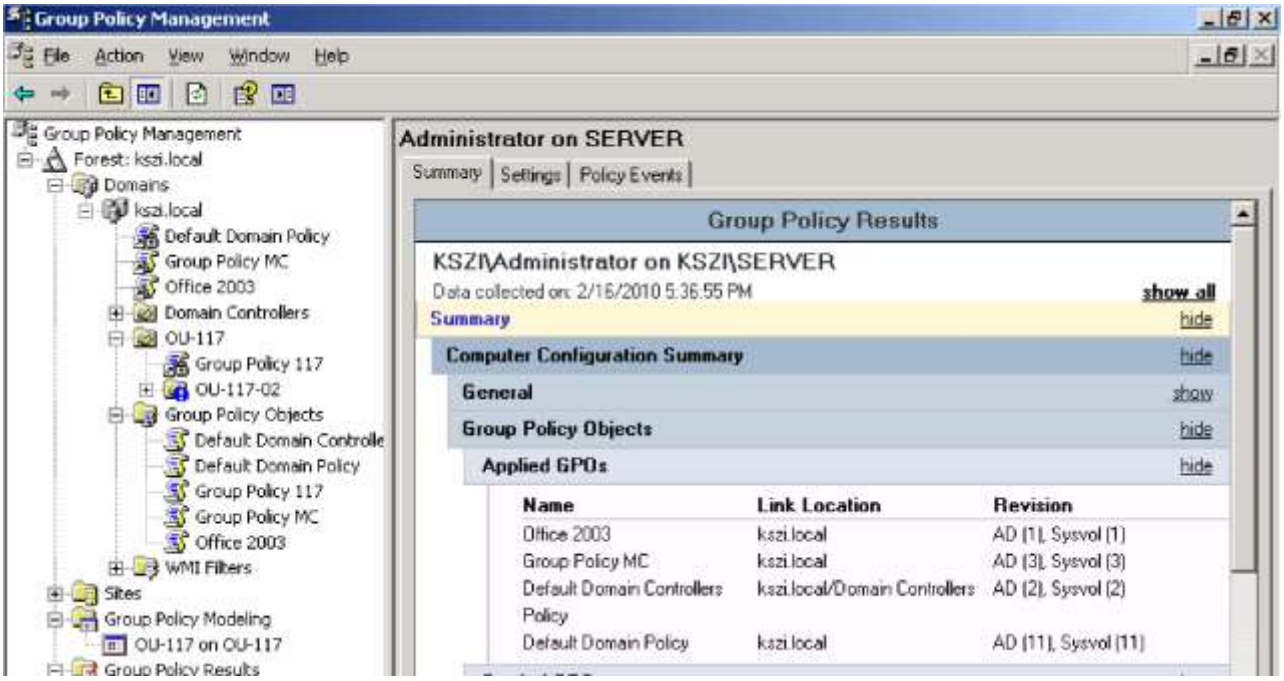

Рис.3.17

Частина 2

Права доступу, спадкування прав доступу, узяття у володіння

Визначення прав доступу до файлових ресурсів здійснюється на основі дозволів (permissions). При визначенні дозволів до ресурсів, наданих у спільний доступ у мережі, використовуються два типи дозволів: мережні дозволи (shared folder permissions) і дозволи, задані у файловій системі NTFS (Ntfs-permissions).

Мережні дозволи

Даний вид дозволів не залежить від типу файлової системи. Мережні дозволи застосовуються тільки при доступі до ресурсів через мережу. Якщо користувач локально ввійшов у систему (локально зареєструвався в системі), те, які б не були призначені мережеві дозволи для певної папки, ці дозволи не будуть застосовуватися ні до самої папки, ні до розміщених у ній файлів. У випадку локальної реєстрації користувача, якщо дані розміщені на томі із системою FAT, користувач має повний доступ до цих даних, якщо дані розміщені на томі NTFS, права доступу будуть визначатися дозволами NTFS.

Надання загального доступу до папки

Надати папку на жорсткому диску в загальне користування можна двома основними способами.

 Відкрити Властивості папки, закладку "Sharing", вибрати пункт "Share this folder"(Рис.3.18):

Рис.3.18

 відкрити оснащення "Shared Folders" у консолі "Computer Managenent", вибрати розділ

"Shares", клацнути правою кнопкою миші й вибрати пункт "New Share…"(Рис.3.19):

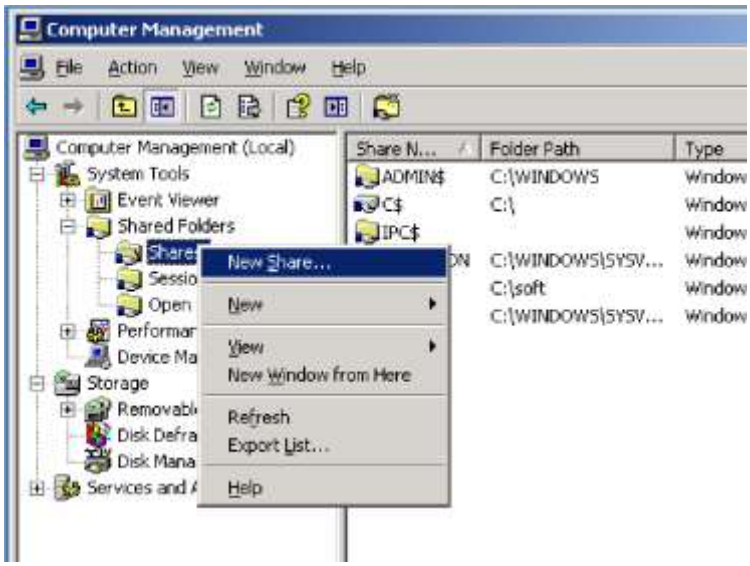

Рис.3.19

 Буде запущений Майстер "Share a Folder Wizard" (Рис.3.20):

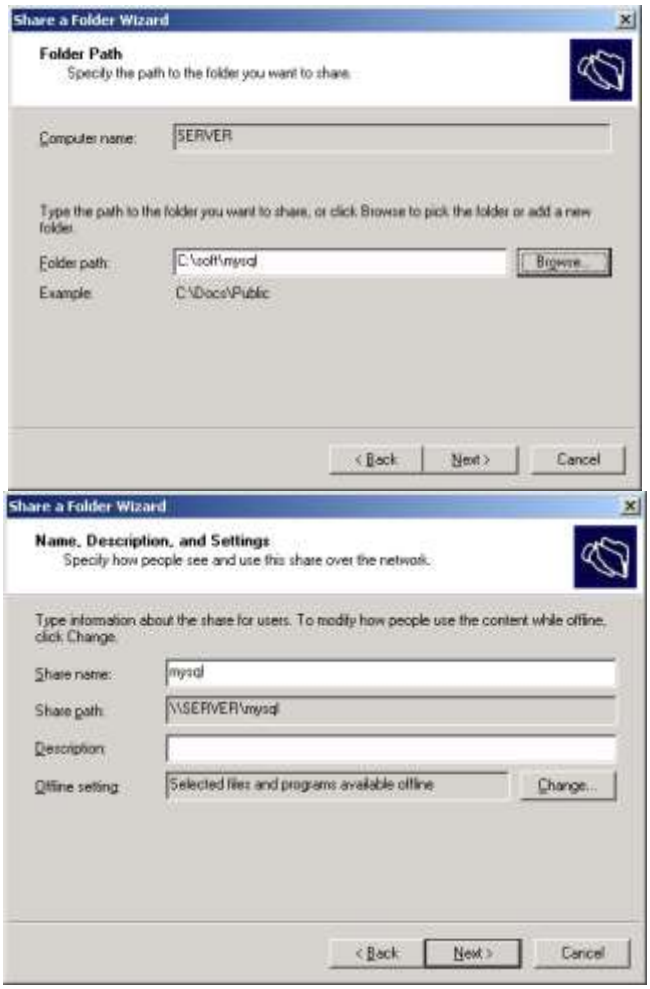

Рис.3.20

Потрібно вказати шлях до папки (увести із клавіатури або знайти за допомогою кнопки "Огляд"), дати назву загальному ресурсу (за замовчуванням ця назва збігається з іменем папки, хоча треба мати на увазі, що не всі додатки можуть сприймати довгі мережні імена із символами не з англійської розкладки.

Далі потрібно задати мережні дозволи на доступ до інформації, що зберігається в даній папці. За замовчуванням призначаються дозволи "Читання" групі "Усі" (Рис.3.21).

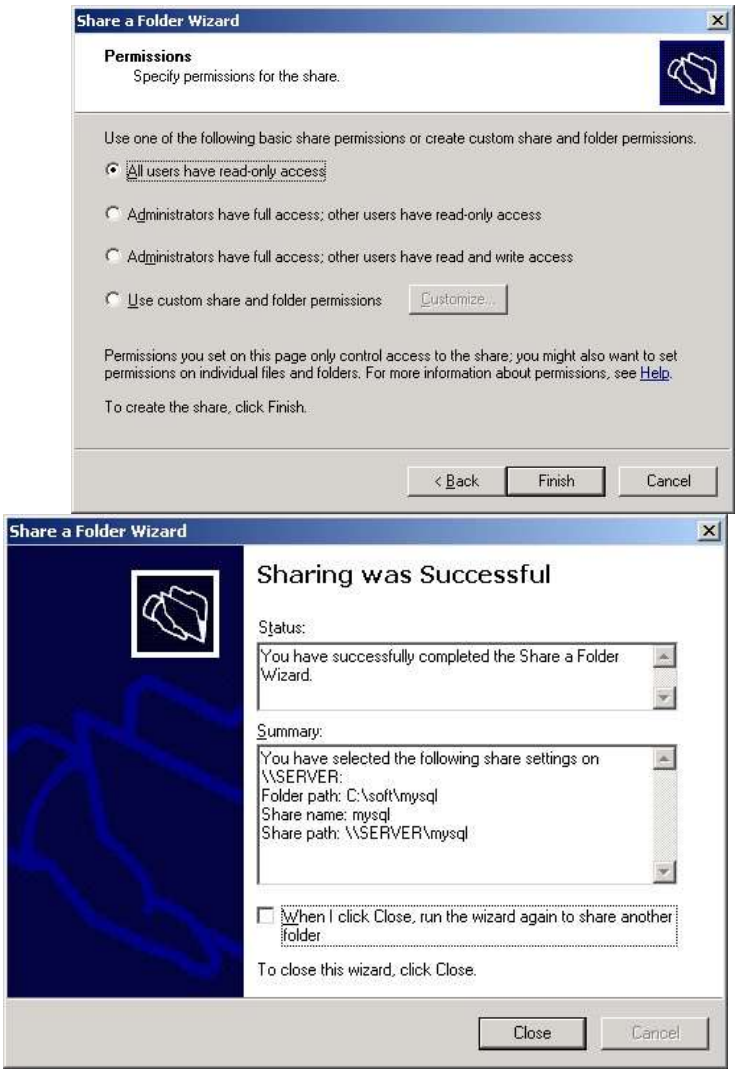

Рис.3.21

Можуть бути призначені мережні дозволи трьох видів:

- Читання (Read) - читання списку файлів і папок, читання даних і запуск програм;
- Зміна (Change) - крім читання даних дозволяє також створювати нові файли й папки, видаляти файли й папки, змінювати дані;
- Повний доступ (Full control) - у додавання до перерахованих вище дозволів можна також змінювати NTFS - Дозволи (якщо загальна папка зберігається на томі NTFS) і одержувати статус власника папки або файлу (теж для томів NTFS).

Визначення сумарних мережних дозволів

Нагадаємо, що при реєстрації користувача домену на якому-небудь комп'ютері контролер домену видає користувачеві т.зв. маркер доступу, який складається з набору ідентифікаторів безпеки (SID) користувача й груп, членом яких він є. Саме цей маркер доступу й визначає, який саме доступ одержить користувач до мережного ресурсу. У тому випадку, якщо якийсь користувач

має дозвіл на доступ до папки по мережі, а також доступ визначений для яких-небудь груп, членом яких він є, то визначення сумарних дозволів проводиться за наступною схемою:

- спочатку перевіряється, чи немає заборон на той або інший вид доступу для користувача й груп, у які він входить, якщо в мережевих дозволах є заборони для користувача або хоча б до однієї із груп, у які він входить, то дані види доступу користувачеві не будуть надані;
- якщо на які-небудь види доступу заборон не має, то діючим дозволом буде найбільший дозвіл, виданий користувачеві або якій-небудь групі, членом якої він є.

Наприклад, у ситуації, зображеної на Рис.3.22 є наступні дозволи:

група "Усі" - "Читання"; користувач User1 - "Читання";
група Group-1 (у яку входить користувач User1) -
"Зміна".

У даній ситуації користувач User1 одержить дозвіл на "Зміну" даних у папці й файлах.

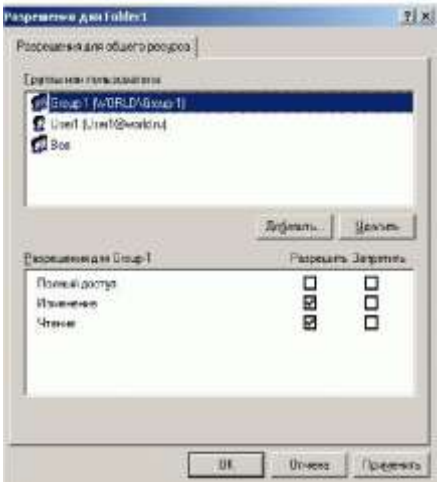

Рис.3.22

Оснащення "Shared Folders" дозволяє також переглядати, хто з користувачів і які саме файли й папки використовує в даний момент (Open Files) (Рис.3.23).

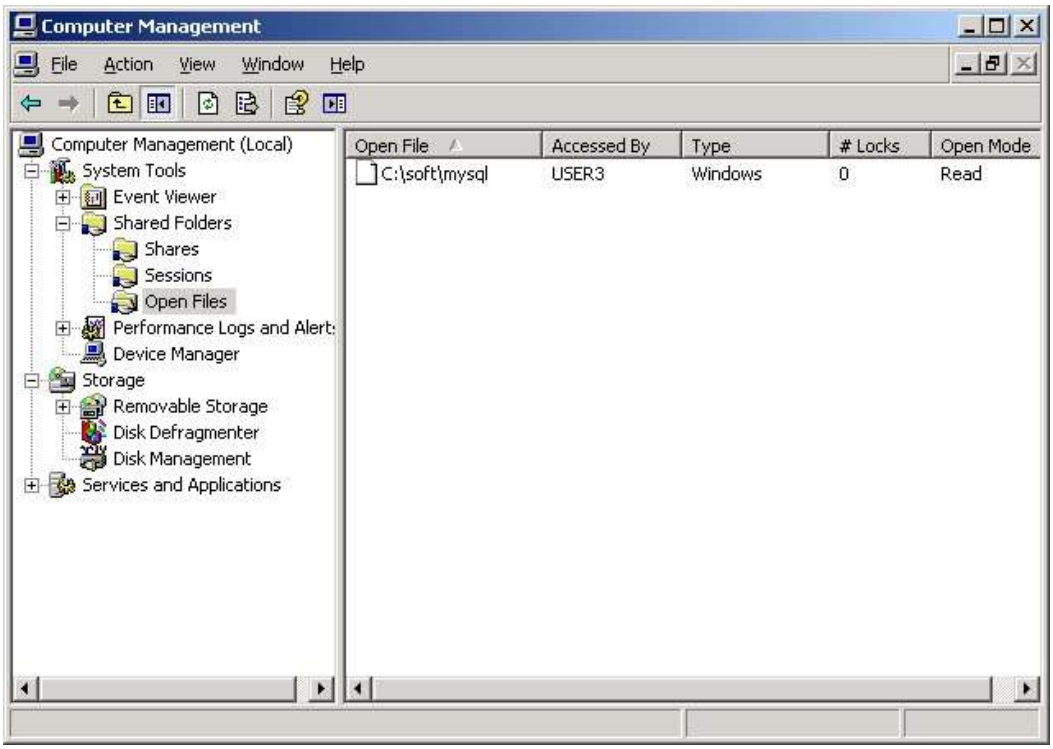

Рис.3.23

Спеціальні мережні ресурси

В будь-якій системі на базі технологій Windows NT існують спеціальні мережні ресурси. Імена деяких ресурсів закінчуються символом $, такі мережні ресурси через "Мережне оточення" або при відкритті ресурсів сервера за допомогою команди "\\<ім'я сервера>" не будуть видні. Проте, якщо вказати повне UNC - ім’я мережного ресурсу, то можна побачити дані, розміщені в ньому.

Перерахуємо ці ресурси :

- ресурс виду "\\<им'я серверу>\admin$" (наприклад, \\Server\admin$) — призначений для віддаленого адміністрування комп'ютера; напрямок завжди відповідає місцю розташування папки, в якій встановлена система Windows; до цього ресурсу можуть підключатися лише члени груп Адміністратори, Оператори архіву і Оператори сервера;
- ресурс вигляду "\\<ім'я сервера>\< буква диску>$" (наприклад \\Server\C$) — коренева папка вказаного диска;. до мережних ресурсів такого типу на сервері Windows можуть підключатися лише члени груп Адміністратори, Оператори архіву і Оператори сервера; на комп'ютерах з Windows XP Professional і Windows 2000 Professional до таких ресурсів можуть підключатися члени груп Адміністратори і Оператори архіву;
- ресурс "\\<ім'я сервера>\IPC$" (наприклад, \\Server\IP$) — використовується для віддаленого адміністрування;
- ресурс "\\<ім'я сервера>\netlogon" (наприклад \\Server\NETLOGON) — використовується лише на контролерах домену, в даній мережній папці зберігаються скрипти (сценарії) для входу користувачів в систему, сумісні з попередніми версіями операційних систем Microsoft;

- ресурс "\\<ім'я сервера>\sysvol" — використовується лише на контролерах домену, в даній мережевій папці зберігається файлова частина групових політик;
- ресурс "\\<ім'я сервера>\print$" — ресурс, який підтримує спільно використовувані принтери, зокрема, в даній папці зберігаються драйвери для спільно використовуваних принтерів.

Проглянути повний список ресурсів, що надаються даним сервером для спільного використання, можна в оснащенні "Shared Folders", в розділі "Shares" (Рис.3.24):

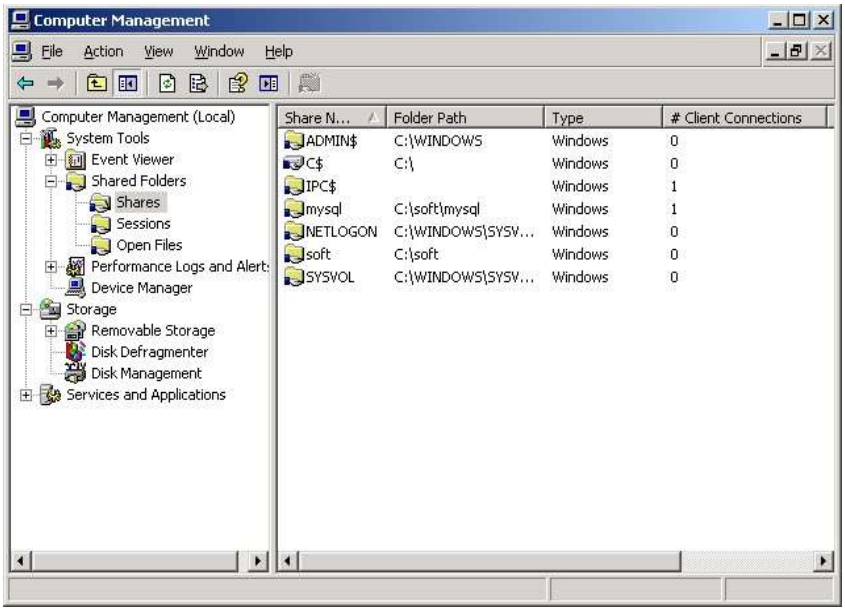

Рис.3.24

У цьому ж розділі даного оснащення можна відключати ресурси від спільного використання в мережі, міняти мережні дозволи, створювати нові мережні ресурси.

Крім спеціальних мережних ресурсів із символом $ наприкінці назви ресурсу, наданих групам з високими повноваженнями, із цим символом можна надати доступ до будь-якого іншого ресурсу, який надається в мережний доступ самим адміністратором. У цьому випадку мережний ресурс також буде схований при звичайному перегляді мережі, але буде доступний при вказівці повного UNC- імені, причому доступ можна дозволити тим групам користувачів, яким потрібний даний ресурс.

Дозволи NTFS

Ще раз підкреслимо, що мережні дозволи діють тільки при доступі до ресурсів через мережу. Якщо користувач увійшов у систему локально, то тепер управляти доступом можна тільки за допомогою дозволів NTFS. На томі (розділі) із системою FAT користувач буде мати повний доступ до інформації даного тому.

Дозвіл NTFS можна встановити, відкривши Властивості папки або файлу й перейшовши на закладку "Безпека" (Security). Набір видів NTFS -дозволів набагато більший, ніж набір мережних дозволів (Рис.3.25).

Рис.3.25

На томі NTFS можна призначати наступні види дозволів для папок:

- Full Control (Повний доступ)
- Modify (Зміна)
- Read & Execute (Читання та виконання)
- List Folder Contents (Список вмісту папки)
- Read (Читання)
- Write (Записування)
- Special Permissions (Особливі дозволи). Для файлів відсутній вид "Читання вмісту папки "(Рис.3.26).

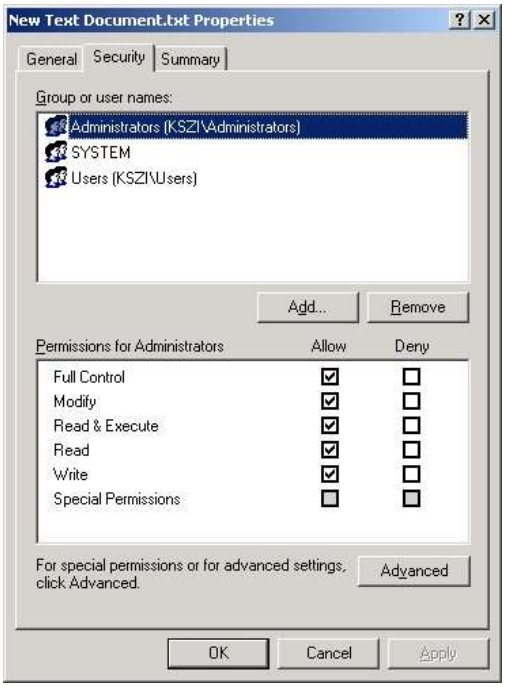

Рис.3.26

Якщо на закладці дозволів нажати кнопку Advanced "Додатково", то можна здійснювати більш тонке настроювання дозволів.

Дозволи NTFS можуть бути явними або успадкованими. За замовчуванням усі папки або файли успадковують дозволи того об'єкта- контейнера (батьківського об'єкта), у якім вони створюються. Використання успадкованих дозволів полегшує роботу з керування доступом. Якщо адміністраторові потрібно змінити права доступу для якоїсь папки й усього її вмісту, то досить зробити це для самої папки й зміни будуть автоматично діяти на всю ієрархію вкладених папок і документів.

Наслідувані повноваження

Якщо ви задаєте повноваження для батьківської папки, то всі файли й папки, створені в даній папці, успадковують ці повноваження. Є три способи, що дозволяють перервати це спадкування:

- Видалення спадкування на рівні батьківської папки, тобто заборона спадкування повноважень дочірніми об'єктами.
- Видалення спадкування на рівні дочірнього об'єкта.
- У дочірньому об'єкті явний дозвіл (allow) або заборона (deny) для певних повноважень із батьківського об'єкта.

У загальному випадку цілком підходять наслідувані повноваження, оскільки їх легко задавати й підтримувати й тому що з ними надійніше працювати, чим з повноваженнями, керування якими відбувається окремо . Якщо вам доводиться змінювати й коректувати наслідувані значення, то, можливо, вам потрібно переглянути організацію папок на сервері. Працюючи з папкою, створюйте підпапки, які логічно повинні містити ті ж повноваження, що й батьківська папка.

Явно обумовлені повноваження й наслідувані повноваження

Явно обумовлені повноваження задаються автоматично операційною системою або вручну адміністратором. Наслідувані повноваження автоматично беруться з батьківської папки як результат спадкування. Є два типи повноважень і що явно задані повноваження мають пріоритет у порівнянні з наслідуваними повноваженнями. Ви, звичайно, розумієте (або повинні зрозуміти), що не зобов'язані переривати ланцюжок спадкування, щоб задати необхідні повноваження дочірньому об'єкту; вам потрібно тільки задати явні повноваження, щоб заборонити/дозволити наслідувані повноваження. Це набагато зручніше (і безпечніше), ніж відмова від простого й надійного принципу наслідуваних повноважень.

Видалення спадкування з батьківського об'єкта

Для зміни настроювання за замовчуванням батьківського об'єкта, щоб дочірні об'єкти не успадковували автоматично повноваження, відкрийте вкладку Security батьківського об'єкту й клацніть на кнопці Advanced. У діалоговім вікні Advanced Security Settings (Додаткові настроювання безпеки) виберіть потрібний елемент (звичайно групу) і клацніть на кнопці Edit. Установіть прапорець Apply These Permissions To Objects And/Or Containers Within This Container Only (Застосовувати ці повноваження до об'єктів і/або контейнерам тільки усередині цього

контейнера). Якщо вам потрібно, то ви можете змінити повноваження, перш ніж заборонити спадкування (Рис.3.27).

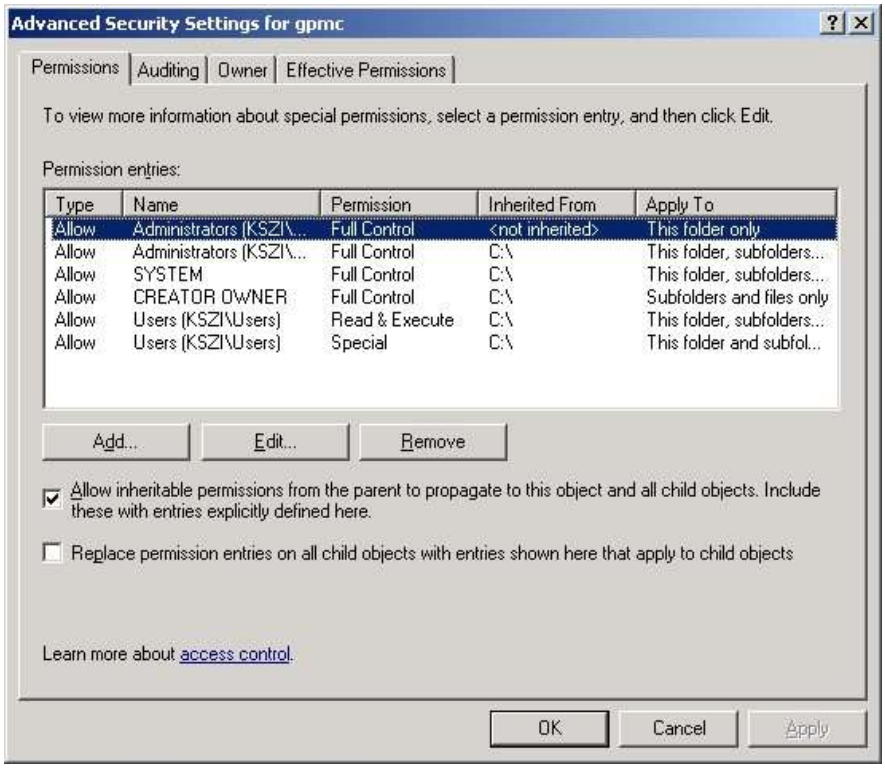

Рис.3.27

Зміна успадкованих повноважень для дочірнього об'єкту

Якщо ви переглядаєте повноваження по батьківському об'єкту, що успадковує повноваження, то відразу звернете увагу, що прапорці для повноважень затінені і недоступні. Ви не можете змінювати повноваження із затіненим прапорцем, але все-таки можете вносити зміни в наслідувані повноваження. Ви могли б, звичайно, вносити зміни в повноваження батьківського об'єкта й потім дочірній об'єкт успадковував би ці повноваження. Але в більшості випадків це нерозумно й навіть небезпечно.

Ви можете вибирати протилежні повноваження (Allow або Deny) для дочірнього об'єкту. У результаті створюються явні повноваження, які заміщують наслідувані повноваження (Рис.3.28).

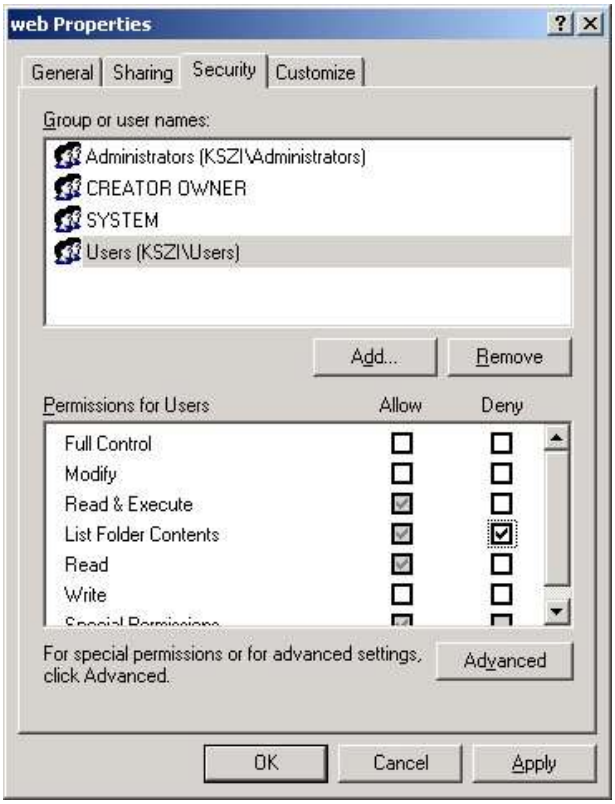

Рис.3.28

Ще один спосіб - це клацнути на кнопці Advanced (Додатково) і вибрати елемент (користувач або група), рівні повноважень якого ви прагнете вилучити зі спадкування. Скиньте прапорець, який указує спадкування (Рис.3.29).

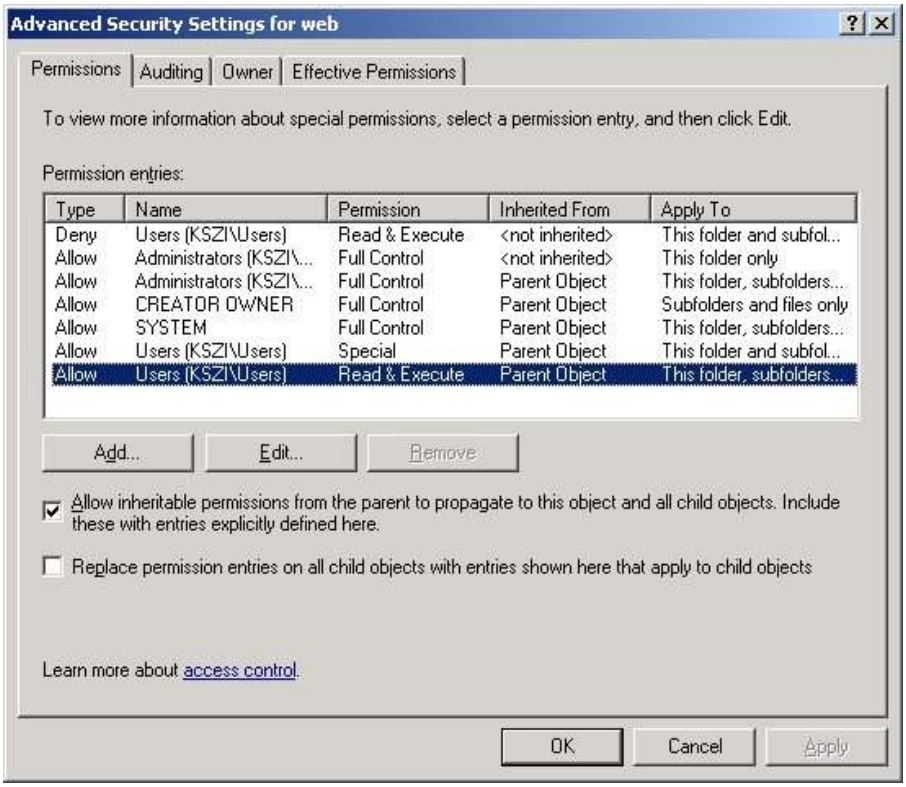

Рис.3.29

Windows виводить діалогове вікно Security, де описується, що означає переривання спадкування й пропонуються наступні три опції(Рис.3.30):

- Copy (Копіювати). Дублювання наслідуваних повноважень, але тепер це явно задані повноваження замість наслідуваних повноважень, тому всі прапорці стають доступні й ви можете змінювати будь-які повноваження.
- Remove. Видалення всіх наслідуваних повноважень, і ви повинні створити явні повноваження.
- Cancel. Скасування вашого рішення.

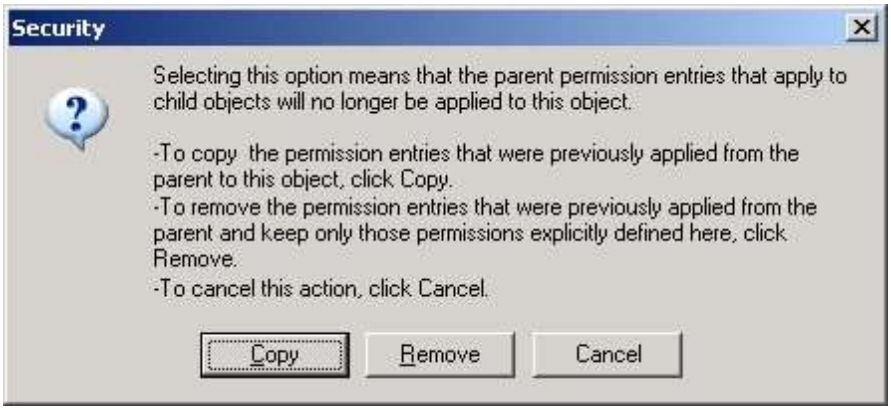

Рис.3.30

Порядок застосування дозволів

Принцип застосування NTFS - Дозволів на доступ до файлу або папки той же, що й для мережних дозволів:

- спочатку перевіряються заборони на які-небудь види доступу (якщо є заборони, то даний вид доступу не дозволяється);
- потім перевіряється набір дозволів (якщо є різні види дозволів для якого-небудь користувача й груп, у які входить даний користувач, то застосовується сумарний набір дозволів).

Але для дозволів NTFS схема небагато ускладнюється. Дозволи застосовуються в наступному порядку:

- явні заборони;
- явні дозволи; успадковані заборони;
- успадковані дозволи.

Якщо SID користувача або SID -и груп, членом яких є даний користувач, не зазначені ні в явних, ні в успадкованих дозволах, то доступ користувачеві буде заборонений.

Володіння папкою або файлом

Користувач, що створив папку або файл, є Власником даного об'єкта. Власник об'єкта має права зміни NTFS - Дозволів для цього об'єкта, навіть якщо йому заборонені інші види доступу. Поточного власника об'єкта можна побачити, відкривши Властивості об'єкта, потім закладку "Безпека", потім нажавши кнопку "Додатково" і перейшовши на закладку "Власник" (Рис.3.31) :

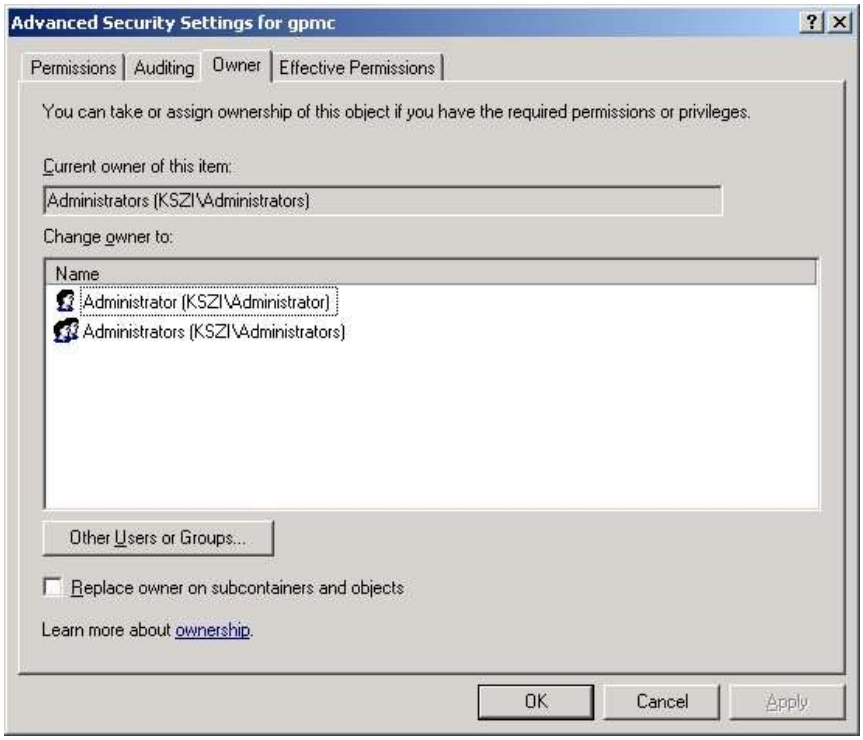

Рис.3.31

Адміністратор системи може змінити власника об'єкта, вибравши нового власника із пропонованого в данім вікні списку або з повного списку користувачів (нажавши кнопку "Інші користувачі або групи"). Ця можливість надана адміністраторам для того, щоб відновити доступ до об'єкта у випадку втрати доступу через неправильно призначені дозволи або видалення облікового запису, що мав винятковий доступ до даного об'єкта.

Спільне використання мережних дозволів і дозволів NTFS

При доступі по мережі до файлових ресурсів, розміщених на томі NTFS, до користувача застосовується комбінація мережних дозволів і дозволів NTFS.

При доступі через мережу спочатку обчислюються мережні дозволи (шляхом підсумовування дозволів для користувача й груп, у які входить користувач). Потім також шляхом підсумовування обчислюються дозволи NTFS. Підсумкові діючі дозволи, надавані до даного конкретного об'єкта, будуть являти собою мінімум з обчислених мережних і NTFS - Дозволів.

Керування доступом за допомогою груп

Групи користувачів створені спеціально для того, щоб більш ефективно управляти доступом до ресурсів. Якщо призначати права доступу до кожного ресурсу для кожного окремого користувача, те, по-перше, це дуже трудомістка робота, і по-друге, ускладнюється відстеження змін у правах доступу при зміні яким-небудь користувачем своєї посади в підрозділі або переході в інший підрозділ.

Для більш ефективного управління доступом рекомендується наступна схема організації надання доступу:

- облікові записи користувачів (accounts) включаються в глобальні доменні групи (global groups) у відповідності зі штатною структурою компанії/організації й виконуваними обов'язками;
- глобальні групи включаються в доменні локальні групи або локальні групи на якомунебудь сервері (domain local groups, local groups) відповідно до необхідних прав доступу для того або іншого ресурсу;
- відповідним до локальних груп призначаються необхідні дозволи (permissions) до конкретних ресурсів.

Дана схема по перших буквах використовуваних об'єктів одержала скорочену назву AGLP (Accounts Global groups Local groups Permissions). При такій схемі, якщо користувач підвищується або знижується на посаді або переходить в інший підрозділ, то немає необхідності переглядати всі мережні ресурси, доступ до яких необхідно змінити для даного користувача. Досить змінити відповідним чином членство користувача в глобальних групах, і права доступу до мережних ресурсів для даного користувача зміняться автоматично.

Додамо, що в основному режимі функціонування домену Active Directory (режими "Windows 2000 основний" або "Windows 2003") з появою вкладеності груп і універсальних груп схема AGLP модифікується в схему AGG…GULL…LP.

Діючі повноваження (Effective Permissions)

В Windows Server 2003 уведена зручна можливість: у вкладці Security діалогового вікна властивостей об'єкта виводяться діючі повноваження для користувачів і груп, які визначені для цього об'єкта. Це не є чимсь новим, і завжди було важливим чинником у визначенні доступу для заданого користувача, але тепер ви можете бачити цю інформацію замість її визначення власними засобами. Діючі повноваження - це "реальні" повноваження, які одержує користувач відповідно до його членства в групах,

Клацніть на кнопці Advanced діалогового вікна Security і перейдіть у вкладку Effective Permissions. Клацніть на кнопці Select, уведіть ім'я користувача або групи й клацніть на кнопці OK. Відповідні прапорці будуть указувати діючі повноваження користувача або групи по цьому об'єкту (Рис.3.32).

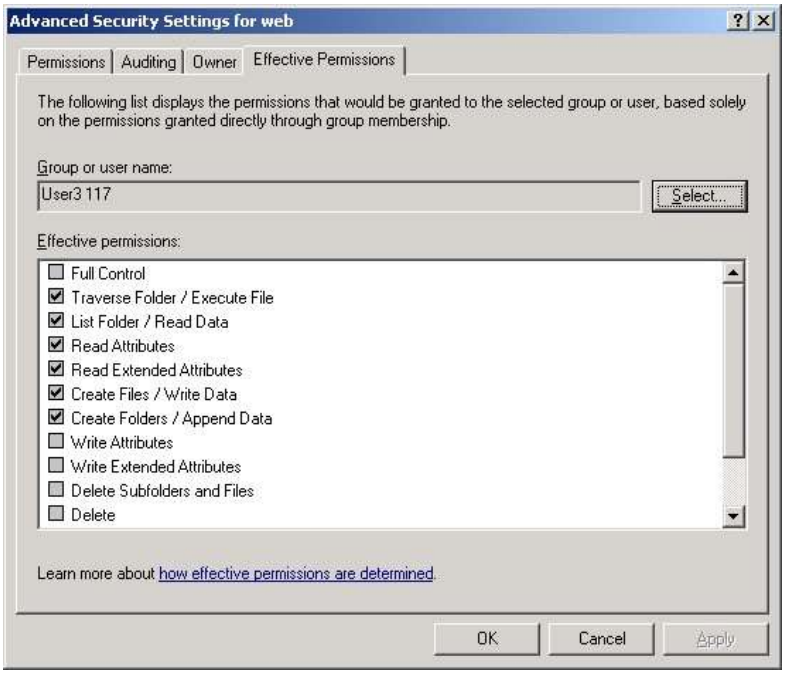

Рис.3.32

Ці повноваження розраховуються з урахуванням членства в групах і наслідуваних повноважень. Система також переглядає всі доменні й локальні групи, у які включений даний користувач або група. Повноваження розділюваного доступу в розрахунках не враховуються.

Аудит доступу до ресурсів

Файлова система NTFS дозволяє здійснювати аудит доступу до файлових ресурсів, тобто відслідковувати й реєструвати події, пов'язані з одержанням або неотриманням доступу до того або іншому об'єкту.

Для того, щоб включити аудит, необхідно виконати дві дії:

- включити політику аудита доступу до об'єктів у домені або тому ОП, у якому розміщений файловий сервер;
- після застосування політики включити аудит доступу на самому об'єкті - папці або файлі.

Перша дія виконується за допомогою редактора групових політик:

- відкриємо розділ "Security Settings" у політиці для відповідного ОП, далі - "Local Policies" і "Audit Policy";
- відкриємо параметр "Audit object access"; включимо механізм аудита для успішного доступу й відмови надання доступу (Рис.3.33).

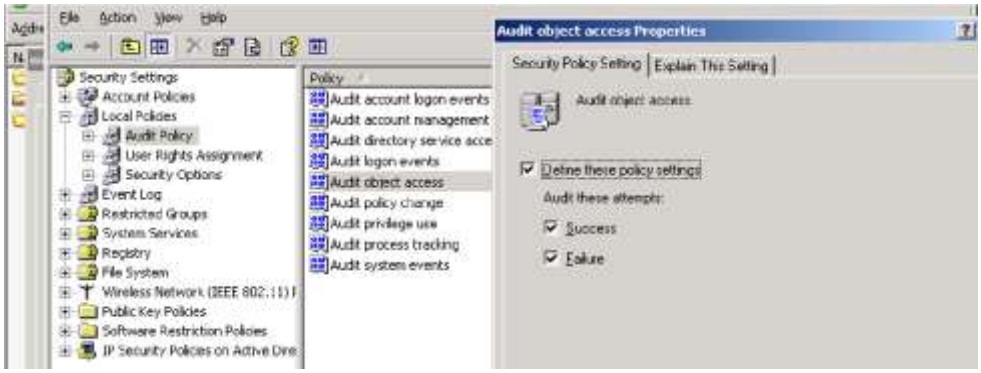

Рис.3.33

Друга дія виконується на закладці "Auditing" після натискання кнопки "Advanced" у параметрах безпеки об'єкта. Потрібно додати списки користувачів і груп, спроби доступу яких будуть відслідковуватися для даної папки або файлу, указавши при цьому, які саме види доступу треба реєструвати. Для того, щоб можна було реєструвати спроби несанкціонованого доступу до файлових ресурсів, необхідно включити в процес реєстрації вдалі, і невдалі спроби доступу (Рис.3.34 а,б).

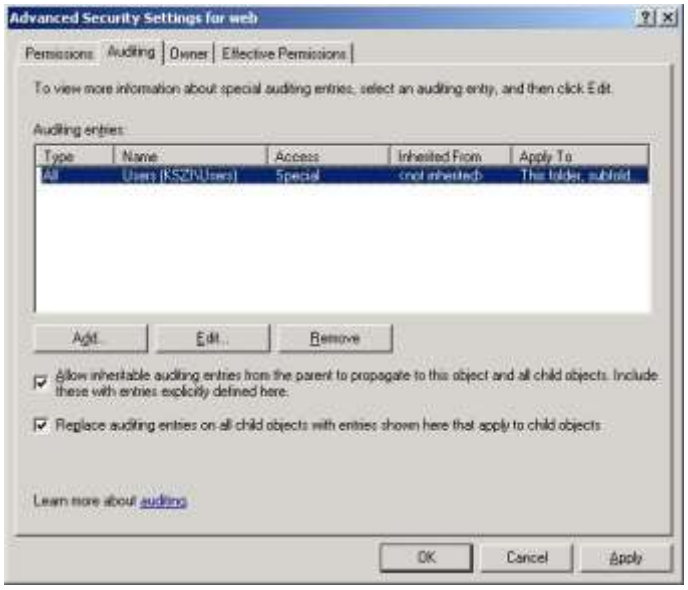

Рис. 3.34 а

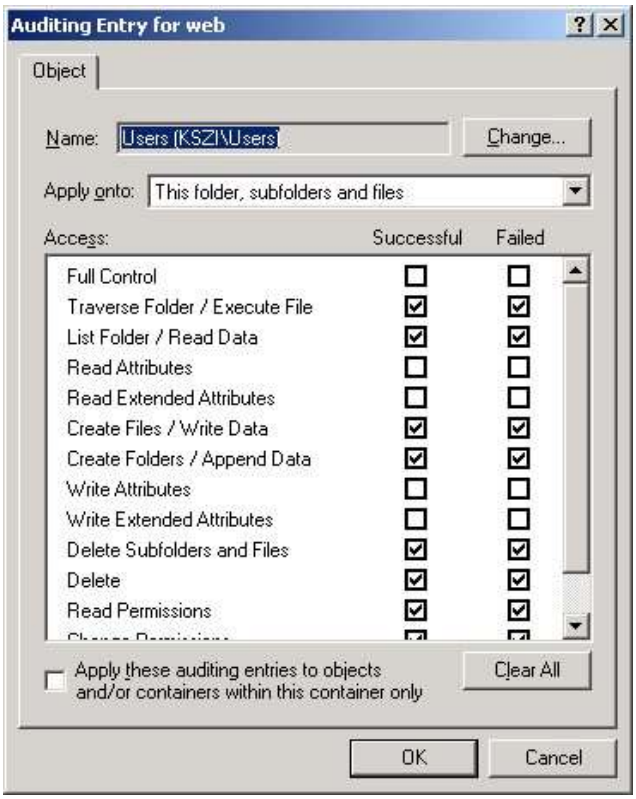

Рис.3.34 б

Після включення механізму аудита всі події доступу, перераховані в настроюваннях аудита, будуть реєструватися в журналі безпеки даного сервера (оснащення "Event Viewer", журнал "Security", категорія "Object Access") (Рис.3.35).

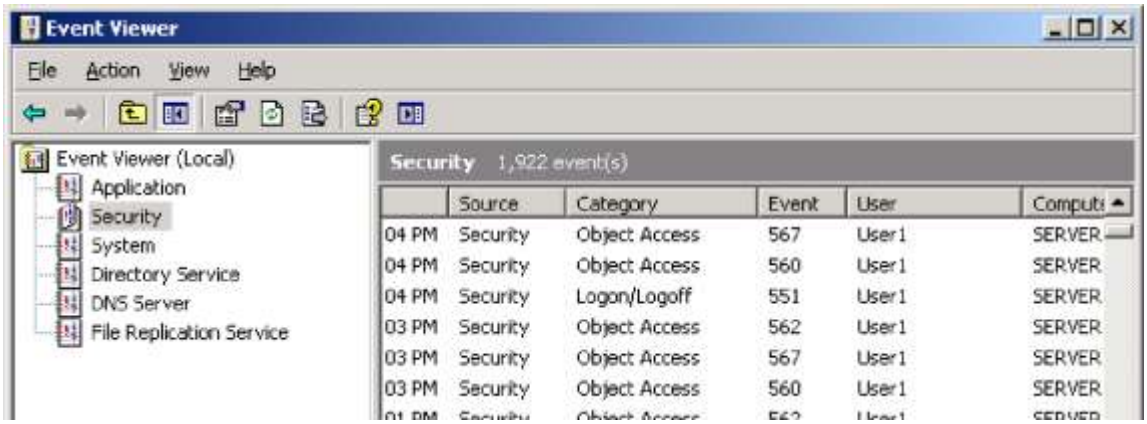

Рис.3.35

У висновку даного пункту відзначимо, що включати аудит великої кількості файлових ресурсів потрібно з великою обережністю. При великій кількості користувачів і оброблюваних ними файлів, якщо включити аудит доступу до файлів, у журналі безпеки буде створюватися дуже багато подій. У випадку якого-небудь інциденту, наприклад, при несанкціонованому доступі до

закритої інформації, знайти потрібний запис буде дуже важко. Тому, перш ніж включити аудит доступу, його необхідно дуже ретельно спланувати.

Необхідно визначити:

- доступ до якої інформації необхідно відслідковувати;
- які види доступу (Читання, Модифікація, Видалення, Зміна дозволів і т.д.);
- типи подій (успішний і неуспішний доступ);
- для яких користувачів необхідно відслідковувати доступ;
- як часто буде проглядатися журнал безпеки; за якою схемою будуть видалятися "старі" події з журналу.

Стиснення і шифрування інформації

Стиснення інформації

Для економії дискового простору можна які-небудь папки або файли зробити стислими. Процес стиснення виконується драйвером файлової системи NTFS. При відкритті файлу в програмі файлова система розпаковує файл, після внесення змін у файл при збереженні на диск файл знову стискається. Робиться це зовсім прозоро для користувача й не доставляє користувачеві ніяких турбот.

Для того, щоб зробити папку або файл стислим, необхідно відкрити сторінку Властивостей відповідної папки або файлу, нажати кнопку "Інші (Advanced)" і поставити галочку в параметрі "Стискати вміст для економії місця на диску (Compress contents to secure data)"(Рис.3.36):

Рис.3.36

Стискати доцільно файли, які при стисненні сильно зменшуються в розмірі (наприклад, документи, створені програмами з пакета MS Office). Не слід стискати дані, які по своїй природі є стислими - наприклад, файли графічних зображень у форматі JPEG, відеофайли у форматі MPEG-4, файли, упаковані програмами- архіваторами (ZIP, RAR, ARJ і інші).

У жодному разі не рекомендується стискати папки з файл - серверними базами даних, тому що такі БД містять велику кількість файлів і при їхньому спільніму використанні багатьма користувачами можуть виникати відчутні затримки, неминучі при розпакуванні файлів, що відкриваються і стисненні файлів, що зберігаються.

Шифрування інформації

Системи сімейства Windows 2000/XP/2003 і більш пізні дозволяють шифрувати дані, що зберігаються на томі із системою NTFS. Шифрування даних здійснюється так само легко, як і їхнє стиснення. Можна замість поля "Стискати вміст…" відзначити галочкою поле "Шифрувати вміст для захисту даних (Encrypt contents to secure data)" (помітимо, що ці два параметри є взаємовиключними - можна в даний момент часу або стиснути дані, або їх зашифрувати)
(Рис.3.37).

Рис.3.37

Шифрування є надійним засобом запобігання несанкціонованого доступу до інформації, навіть якщо буде викрадено комп'ютер із цією інформацією або жорсткий диск із комп'ютера. Якщо дані зашифровані, то доступ до них має (з невеликим виключенням) тільки той користувач, який виконав шифрування, незалежно від установлених дозволів NTFS. Шифрування проводиться компонентом "Шифрована файлова система" (EFS, Encrypted File System), що є складовою частиною файлової системи NTFS.

Процес шифрування проводиться за наступною схемою:

- при призначенні файлу атрибута "Зашифрований" драйвер системи EFS генерує "Ключ шифрування файлу" (FEK, File Encryption Key);
- блоки даних файлу послідовно шифруються за симетричною схемою (одним з алгоритмів симетричного шифрування, вбудованих у систему);
- ключ шифрування файлу (FEK) шифрується за асиметричною схемою відкритим ключем агента відновлення (RA, Recovery Agent); зашифрований ключ шифрування файлу зберігається в атрибуті файлу, названим "Поле відновлення даних" (DRF, Data Recovery Field).

Поле відновлення даних необхідно для захисту від втрати доступу до зашифрованої інформації в тому випадку, якщо буде видаленній (разом із ключем шифрування даних) обліковий запис користувача, що зашифрував ці дані. Агент відновлення - це спеціальний обліковий запис, для якого EFS створює т.зв. "сертифікат агента відновлення", до складу якого входять відкритий і закритий ключі цього агента. Особливість асиметричного шифрування полягає в тому, що для шифрування й дешифрування даних використовуються два ключі - одним ключем дані шифруються, іншим дешифруються. Відкритий ключ агента відновлення доступний будь-якому користувачеві, тому, якщо користувач шифрує дані, то в зашифрованих файлах завжди присутнє поле відновлення даних. Закритий ключ агента відновлення доступний тільки обліковому запису цього агента. Якщо ввійти в систему з обліковим записом агента відновлення зашифрованих даних, то при відкритті зашифрованого файлу спочатку розшифровується закритим ключем агента відновлення, що зберігається в DRF, ключ шифрування даних, а потім уже витягнутим ключем шифрування дешифруються самі дані.

За замовчуванням агентом відновлення на кожному окремо взятому комп'ютері є локальний обліковий запис Адміністратор даного комп'ютера. У масштабах домену можна встановити службу сертифікатів, згенерувати для певних доменних облікових записів відповідні сертифікати, призначити ці облікові записи агентами відновлення (за допомогою групових політик) і встановити ці сертифікати на тих файлових серверах, на яких необхідно шифрувати дані. При використанні в масштабах корпоративної мережі технології шифрування даних слід попередньо спланувати всі ці дії (розгортання служб сертифікатів, видача й зберігання сертифікатів, призначення агентів відновлення, процедури відновлення даних у випадку видалення облікового запису, за допомогою якого дані були зашифровані).

Слід також пам'ятати, що дані зберігаються в зашифрованому виді тільки на жорсткому диску. При передачі по мережі дані передаються із сервера на ПК користувача у відкритому виді (якщо не включені політики Ipsec).

ПРАКТИЧНЕ ЗАВДАННЯ

1.Створення Організаційних підрозділів, розміщення в ОП користувачів і груп

- Створіть Організаційний підрозділ (OU) з іменем OU-117
- Створіть в OU-117 користувача User1-117, User1-117-01,User2-117-01

- У підрозділі OU-117 створіть підрозділи OU-117-01, OU-117-02
- Перемістіть користувачів User1-117-01,User2-117-01 у підрозділ OU-117-01
- Створіть в OU-117-02 користувача User2-117-02
- Створіть у підрозділі OU-117 групи Group1-117, Group2-117
- Перемістіть в групи Group1-117 користувачів підрозділу OU-117-01, а в Group2-117 користувачів підрозділу OU-117-02

2. Делегування адміністративних повноважень

- Надайте адміністративні права на OU-117 користувачеві User1-117.
- Увійдіть у систему як User1-117, спробуйте змінити властивості користувачів в OU-117 і OU-117-02, створити в них нових користувачів або групи користувачів
- Спробуйте зробити те ж саме в домені за межами цих підрозділів

3.Створення об'єкта групової політики, настроювання параметрів ГП (обмеження інтерфейсу користувача) Створіть Групову політику для ОП OU-117 (Рис.3.38).

Рис.3.38

- Призначте в цій політиці обмеження інтерфейсу для користувачів (кнопка Edit). Ввімкніть параметри:
  - "User Configuration"/ "Administrative Templates"/ "Windows Components"/ "Windows Explorer"/ "Remove File Menu from Windows Explorer"
  - "User Configuration"/ "Administrative Templates"/ "Windows Components"/ "Windows Explorer"/ "Remove Search Button from Windows Explorer"

- "User Configuration"/ "Administrative Templates"/ "Start Menu and Taskbar"/ "Remove Search Menu from Start Menu" - "User Configuration"/ "Administrative Templates"/ "Start Menu and Taskbar"/ "Remove Run Menu from Start Menu "
- "User Configuration"/ "Administrative Templates"/ "Desktop"/ "Remove My Documents icon on the desktop"
- "User Configuration"/ "Administrative Templates"/ "Desktop"/ "Remove My Computer icon on the desktop"
- "User Configuration"/ "Administrative Templates"/ "Desktop"/ "Hide Internet Explorer icon on desktop"

 Увійдіть у систему як User1-117, User1-117-01, User2-117-02, проаналізуйте зміни інтерфейсу

4. Обмеження прав доступу до об'єкта ГП

 Увійдіть у систему як Administrator, забороніть читання й застосування об'єкта ГП підрозділу OU-117 для користувача User1-117:

- Відкрийте вікно Properties для GroupPolicy117, далі перейдіть у вкладку Security (якщо вкладка Security не відображається, ввімкніть Advanced Features в меню View консолі AD Users and Computers) (Рис..3.39)

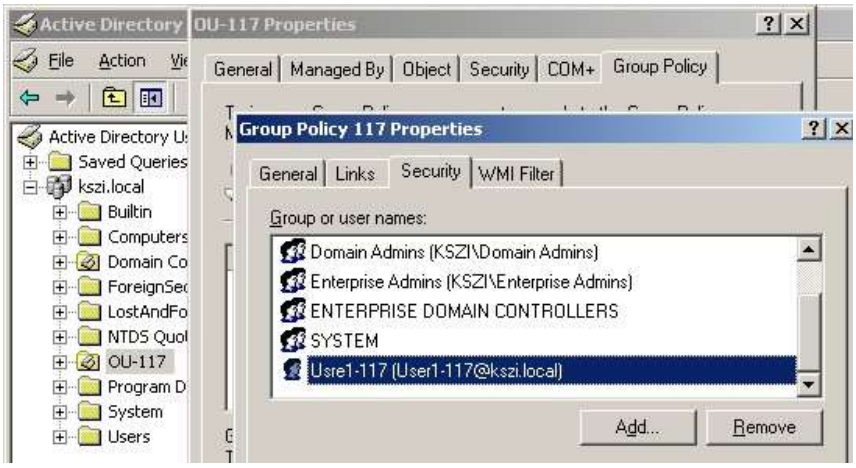

Рис..3.39

- У вікні "Permissions for User1-117" поставити галочки в стовпці "Deny" для дозволів "Read" і "Apply Group Policy"(Рис.3.40).

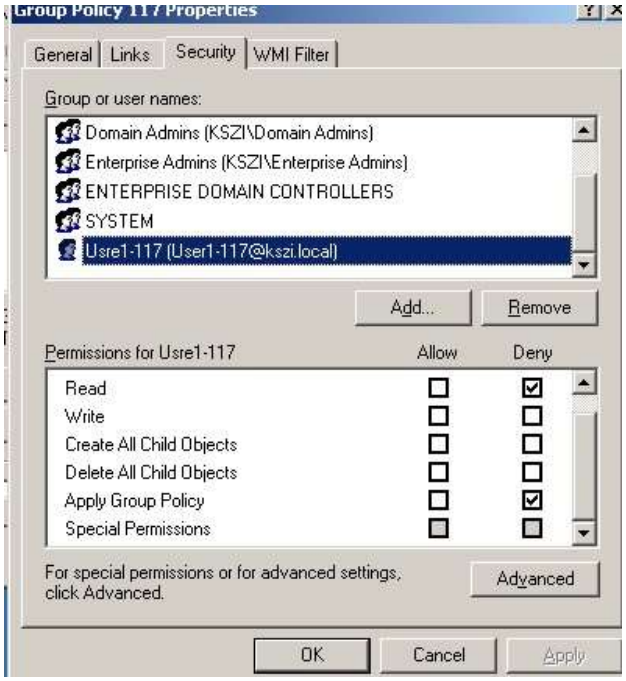

Рис.3.40

 Увійдіть у систему як User1-117, User2-117-02, проаналізуйте зміни інтерфейсу

Увійдіть у систему як Administrator, поверніть вихідні значення дозволів для політики GroupPolicy117

5. Блокування спадкування групових політик

 Увійдіть у систему як User1-117, установіть блокування групових політик для OU-117-02 (Рис.3.41).

Рис.3.41

У вікні Properties для OU-117-02 закладка "Group Policy" - поставити галочку в поля "Block Policy Inheritance"

- Увійдіть у систему як User1-117-01, User2-117-02, проаналізуйте зміни інтерфейсу

6. Примусове застосування групових політик

- Увійдіть у систему як Administrator, забороніть блокування політик на рівні OU-117 (Рис..3.42).

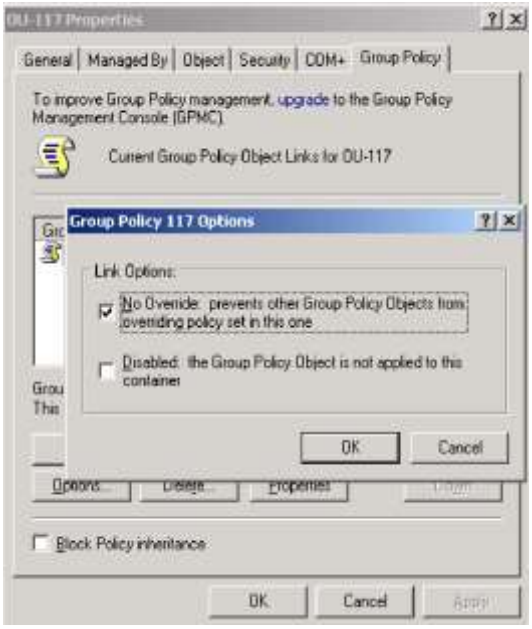

Рис..3.42

У вікні Properties для OU-117 закладка "Group Policy" - кнопка "Options…" - поставити галочку в поле "no Override: prevents other Group Policy Objects from overriding policy set in this one" ("Не перекривати: інші об'єкти групової політики не можуть перекривати параметри цієї політики")

- Увійдіть у систему як User1-117-01, User2-117-02, проаналізуйте зміни інтерфейсу

7. Створення об'єкта групової політики для призначеного пакета програмного забезпечення:

- Створіть Групову політику для вашого домену "Group Policy MC"
- Настройте параметри для установки пакета ПО (пакет GPMC - Group Policy Management Console) (Рис.3.43).

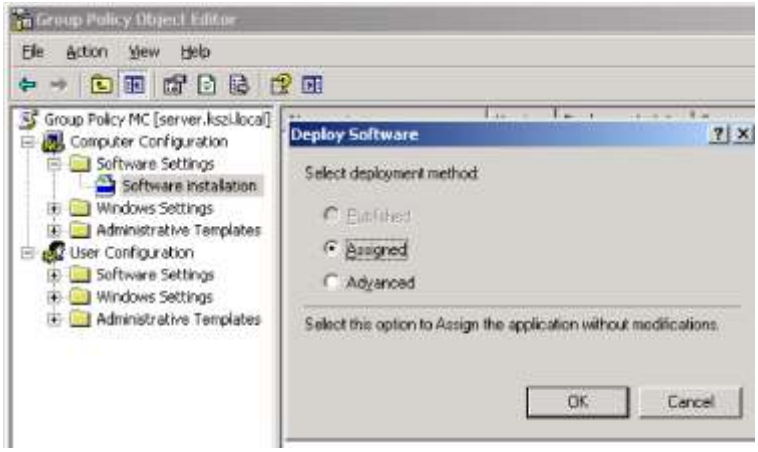

Рис.3.43

У розділі "Computer Configuration", "Software Settings", "Software installation" , "new - Package…" Вказуємо шлях до пакета (наприклад, "\\SERVER\soft\gpmc\gpmc.msi") і Режим - "Assigned"

Примітка: На одному із серверів домену в папці із загальним доступом попередньо повинен бути розміщений пакет, що встановлюється.

- Застосуйте нові політики (gpupdate)
- Перезавантажити сервер
- У процесі завантаження системи й застосування політик відбудеться установка пакета GPMC. Простежте установку пакета для сервера домену й клієнтів.

8. Створення об'єкта групової політики для публічного пакета програмного забезпечення

 Створіть Групову політику для вашого домену "Group Policy MS Office 2003" Настройте параметри для установки пакета ПО (пакет MS Office 2003 Professional)(Рис.3.44):

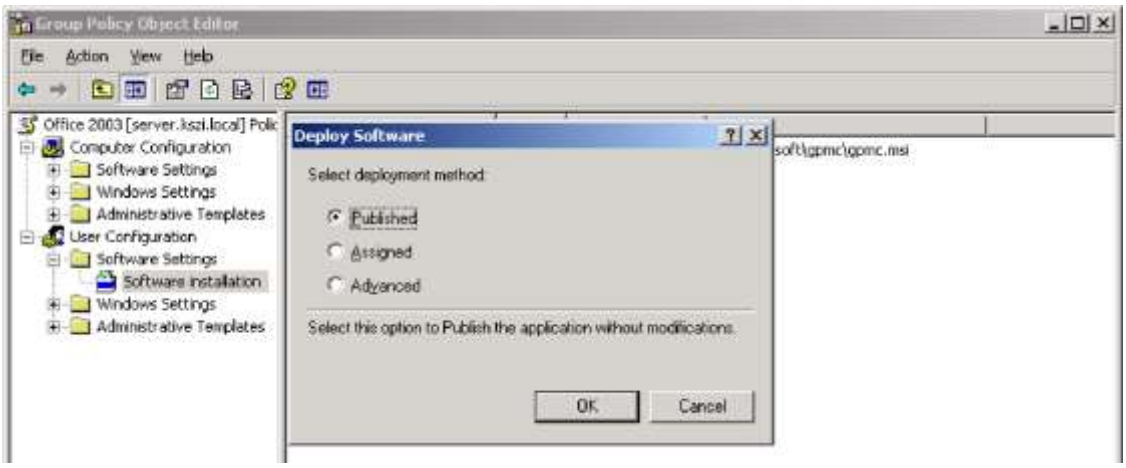

Рис.3.44

У розділі "User Configuration", "Software Settings", "Software installation" , "new - Package…" Вказуємо шлях до пакета (наприклад, "\\SERVER\soft\OFFICEPRO2003 \PRO11.MSI") і Режим - "Published"

Примітка: На одному із серверів домену в папці із загальним доступом попередньо повинен бути розміщений пакет, що встановлюється.

- Застосуйте політики: у командному рядку ввести команду gpupdate
- Перевірте, що пакет MS Office 2003 доступний для встановлення на сервері і клієнті домену:

Відкрийте Панель керування - "Установка й видалення програм" - Кнопка "Установка програм". У вікні "Додавання програм з вашої мережі" повинен з'явитися доступний для установки пакет MS Office 2003.

Примітка: У вправі 8 у якості пакета ПО для установки можна використовувати будь-який програмний продукт, для якого є встановлюючий файл у форматі ".msi"

9. Керування груповими політиками за допомогою консолі Group Policy Management Console

Відкрийте консоль GPMC

Вивчіть керування політиками за допомогою даної консолі:

- встановіть покажчик миші на різних об'єктах AD (домен, Організаційні підрозділи), перегляньте списки об'єктів ГП, прив'язаних до обраних об'єктів AD; розкрийте контейнер Group Policy Objects, перегляньте повний список ГП у вашому домені;
- у цьому ж списку відкрийте який-небудь об'єкт ГП для редагування (клацнути правою кнопкою миші на об'єкті ГП, вибрати Edit);

- створіть резервну копію об'єкта ГП на жорсткому диску (клацнути правою кнопкою миші на об'єкті ГП, вибрати Back Up, нажати кнопку "Огляд" (Browse), вибрати папку для збереження резервної копії ГП, кнопка "ОК ", кнопка Back Up, кнопка "ОК", відкрийте дану папку, перегляньте файл із резервною копією об'єкта ГП - файл manifest.xml) Закрийте консоль GPMC.

10. Локальні права доступу із забороною доступу (дозволи NTFS)

- Створіть папку на розділі NTFS (наприклад, папку Folder на розділі C:). Розмістіть в ній різні документи (файли).
- Призначте локальні права доступу до папки Folder:
  Група "Everyone" – Allow Full Control
  Група "Group1-117" - Denny Full Control
- Перевірте доступ до папки для користувача User1-117-01:
  - увійдіть у систему як користувач User1-117-01;
  - спробуйте відкрити папку Folder і розміщені в ній документи.

- Перевірте доступ до папки для користувача User2-117-02:
  - увійдіть у систему як користувач User2-117-02;
  - спробуйте відкрити папку Folder і розміщені в ній документи.

11. Локальні права доступу (дозволи NTFS)

- Призначте локальні права доступу до папки Folder:
  Вилучити групу "Everyone"
  Група Group1-117 - Allow Read
  Група Group2-117 – Allow Modify
- Перевірте доступ для користувача User1-117-01 увійдіть у систему як користувач User1-117-01;
  спробуйте відкрити папку Folder і розміщені в ній документи; спробуйте змінити наявні документи; спробуйте створити нові документи.
- Перевірте доступ для користувача User2-117-02 увійдіть у систему як користувач User2-117-02;
  спробуйте відкрити папку Folder і розміщені в ній документи; спробуйте змінити наявні документи; спробуйте створити нові документи.

12. Мережні й локальні права доступу

- Відкрийте мережний доступ до папки Folder

- Мережні дозволи: Група " Everyone " – Allow Read
- Перевірте різницю між доступ до папки і її вмісту при доступі через мережу (наприклад, \\SERVER\Folder) і локально (наприклад, C:\Folder) від імені Administrator чи User2-117-02

13. Узяття у володіння файлових ресурсів

- Увійдіть у систему як користувач User1-117
  - Створіть папку
  - Відкрийте Властивості папки
  - Перейдіть на закладку "Security"
  - Натисніть кнопку "Advansed"
  - заберіть галочку в поля "Дозволити спадкування дозволів від батьківського об'єкта до цього об'єкта ... (Allow inheritable permissions……)"
  - у панелі, що з'явився, натисніть кнопку "Remove"
  - далі кнопка "ОК" - на запитання "Do you want to continue?" кнопка "Yes"(Рис.3.45)

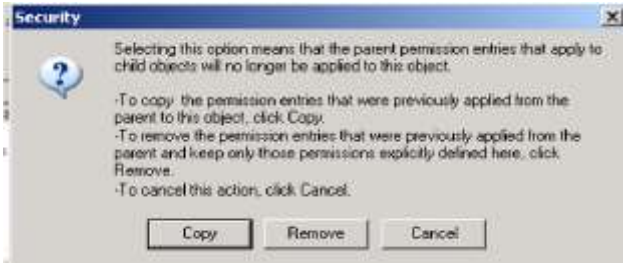

Рис.3.45

 натисніть кнопку "Додати" і додайте користувача User1-117;

 призначте права доступу " Allow Full Control " ; кнопка ОК (Рис.3.46).

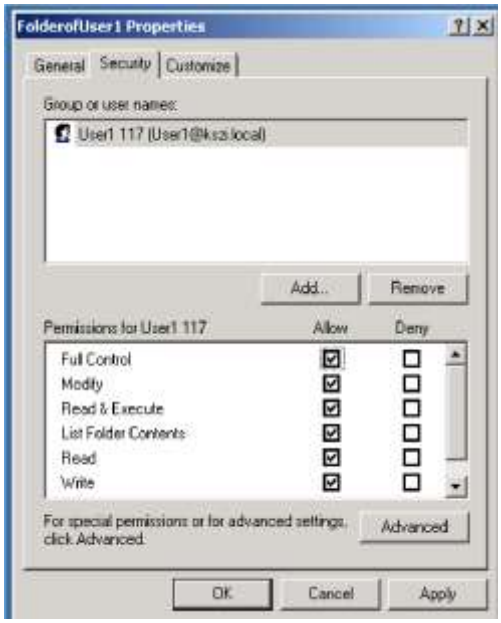

Рис.3.46

- Увійдіть у систему як Адміністратор
  - Спробуйте відкрити створену користувачем User1-117 папку й розміщені в ній документи

  - Відкрийте Властивості папки
  - Перейдіть на закладку "Security"
  - натисніть кнопку "Advanced"
  - відкрийте закладку "Owner"
  - виберіть у списку групу "Administrators"
  - поставте галочку в полі "Змінити власника підконтейнерів і об'єктів (Replace owner …)" (Рис..3.47)

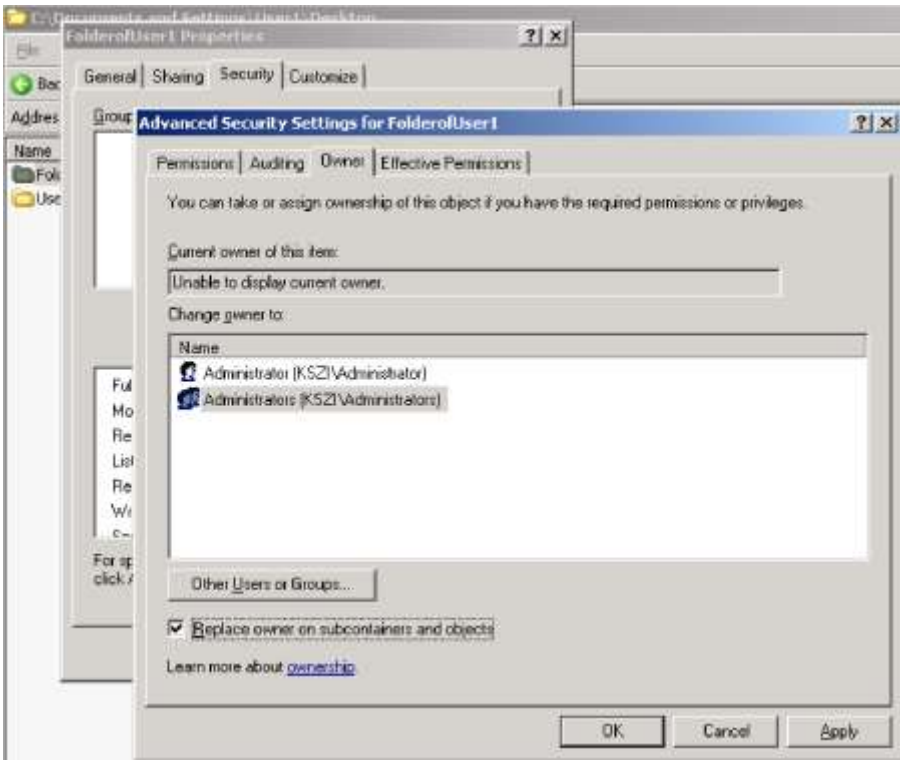

Рис.3.47

- Кнопка "ОК "
- Кнопка "Yes"
- Кнопка "ОК "

- Відкрийте Властивості папки. Перейдіть на закладку "Security"
- У списку доступу до папки, що з'явився, додайте групу "Administrators" призначте права доступу цій групі "Full Control" - кнопка "ОК" (Рис.3.48)

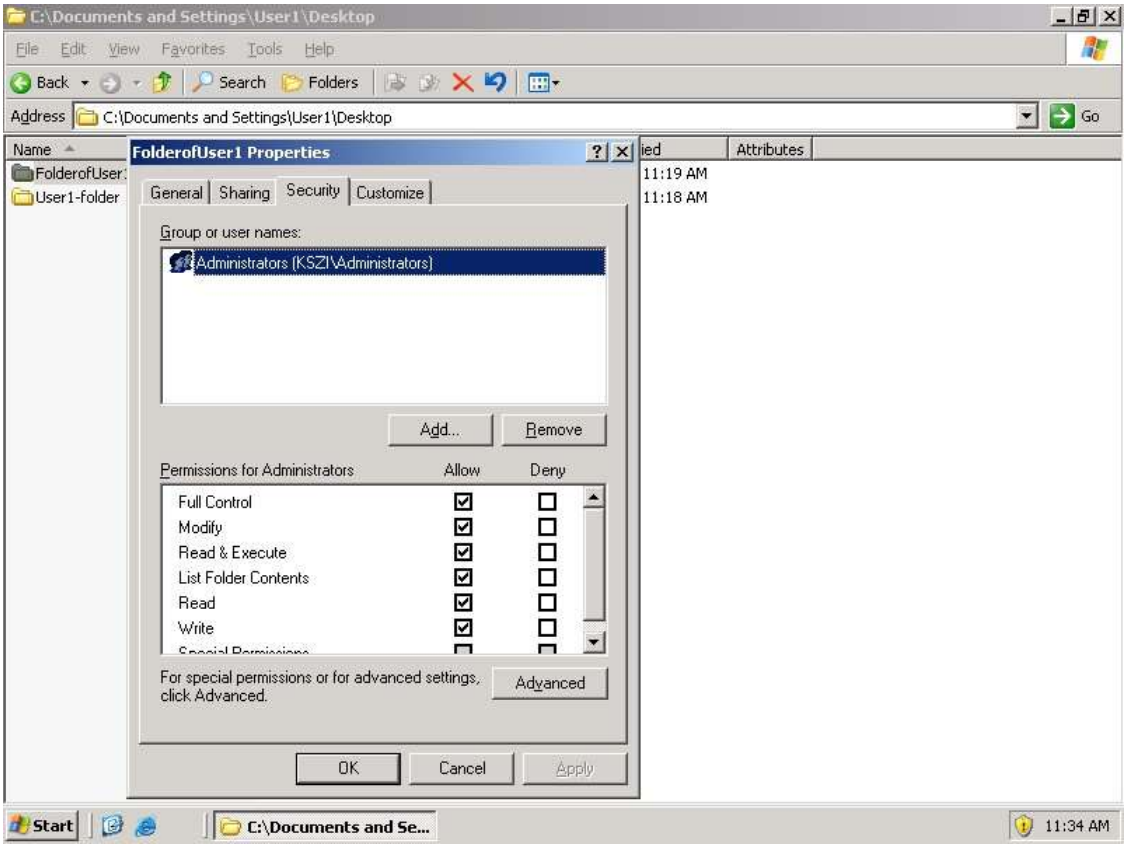

Рис..3.48

 Знову спробуйте відкрити дану папку й розташовані в ній документи.

14. Стиснення даних на диску

- Увійдіть у систему як Адміністратор
- Відкрийте Властивості папки "C:\Folder"
- На закладці "General" натисніть кнопку "Advanced…"
- У розділі "Compress or Encrypt attributes" поставте галочку в поля "Compress contents to save disk space"(Рис.3.49)

Рис.3.49

 Знову відкрийте Властивості папки, порівняєте поля "Size" і "Size on Disk" (Рис.3.50)

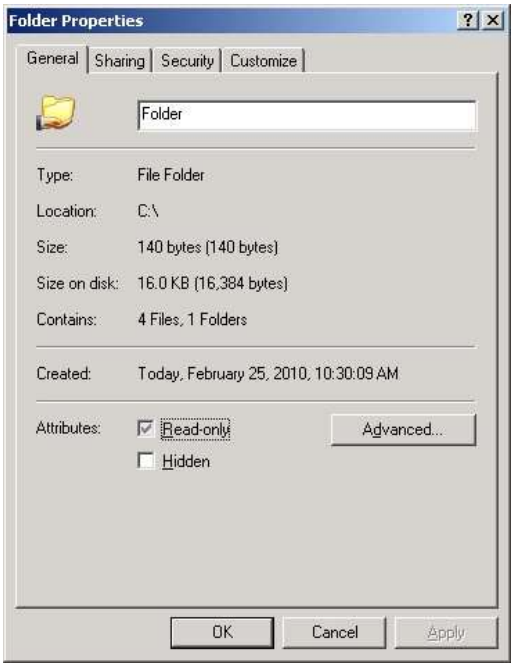

Рис.3.50

15. Шифрування даних

- Відкрийте Властивості папки "C: \Folder"
- На закладці "General" натисніть кнопку "Advanced…"
- У розділі "Compress or Encrypt attributes" поставте галочку в полі "Encrypt contents to secure data"
- Увійдіть у систему як User1-117
- Спробуйте відкрити папку й розміщені в ній документи.
- Увійдіть у систему як Адміністратор
- Відключіть шифрування папки

16. Включення політики аудита

- Увійдіть у систему як Адміністратор
- Запустіть консоль "Domain Controller Security Policy"
- Далі: "Security Settings" - "Local Policies" - "Audit Policy" Відкрийте параметр "Audit object access " - Поставте галочки в обох полях "Success" і "Failure" (Рис.3.51)

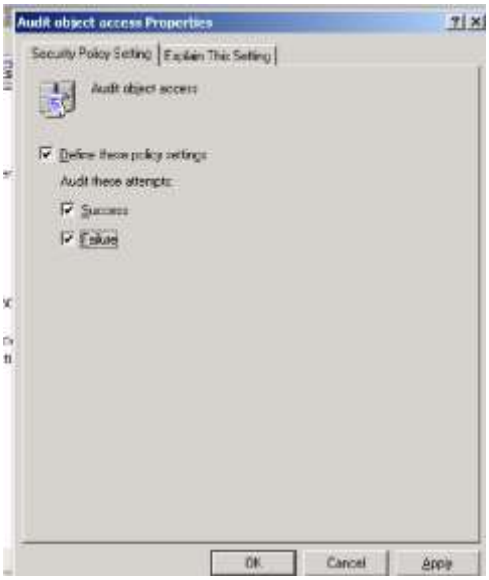

Рис.3.51

17. Включення аудита доступу до файлів для конкретної папки

 Відкрийте Властивості папки "C:\Folder"

 Далі:

- Закладка "Security"
- Кнопка "Advanced" Закладка"Auditing"
- Кнопка "Add"
- Додайте групу "Users"
- Кнопка "ОК "
- Поставте галочки в стовпцях "Successful" і "Failed" для рядків "Read Data", "Delete Subfolders and Files"
- натисніть кнопку "ОК " потрібне число раз(Рис.3.52)

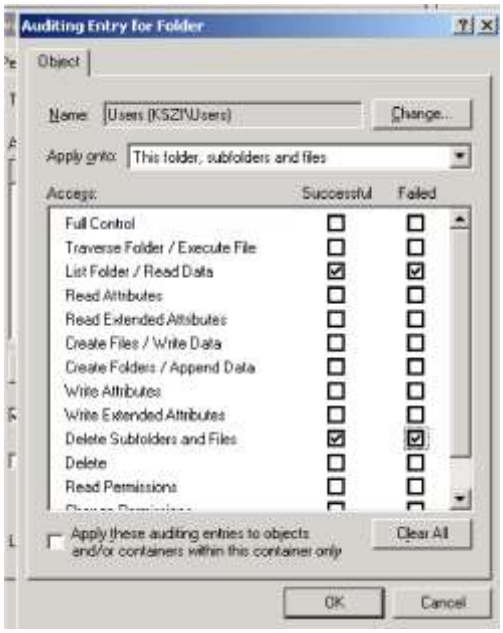

Рис.3.52

18. Тестування аудита доступу до файлів

- Увійдіть у систему як Адміністратор і як User1-117
- Відкрийте папку "C:\Folder"
- Спробуйте відкривати розміщені в папці файли
- Спробуйте вилучити розміщені в папці файли
- Увійдіть у систему як Адміністратор
- Відкрийте консоль "Event Viewer"(Рис..3.53)
- Відкрийте журнал "Security"
- Вивчіть записи журналу з категорії "Object Access"(Рис..3.54)

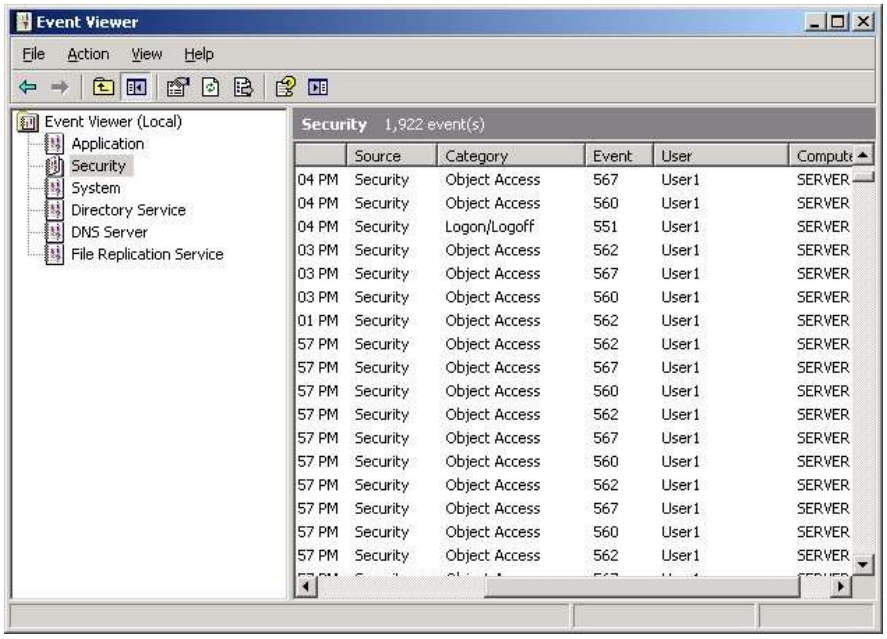

Рис.3.53

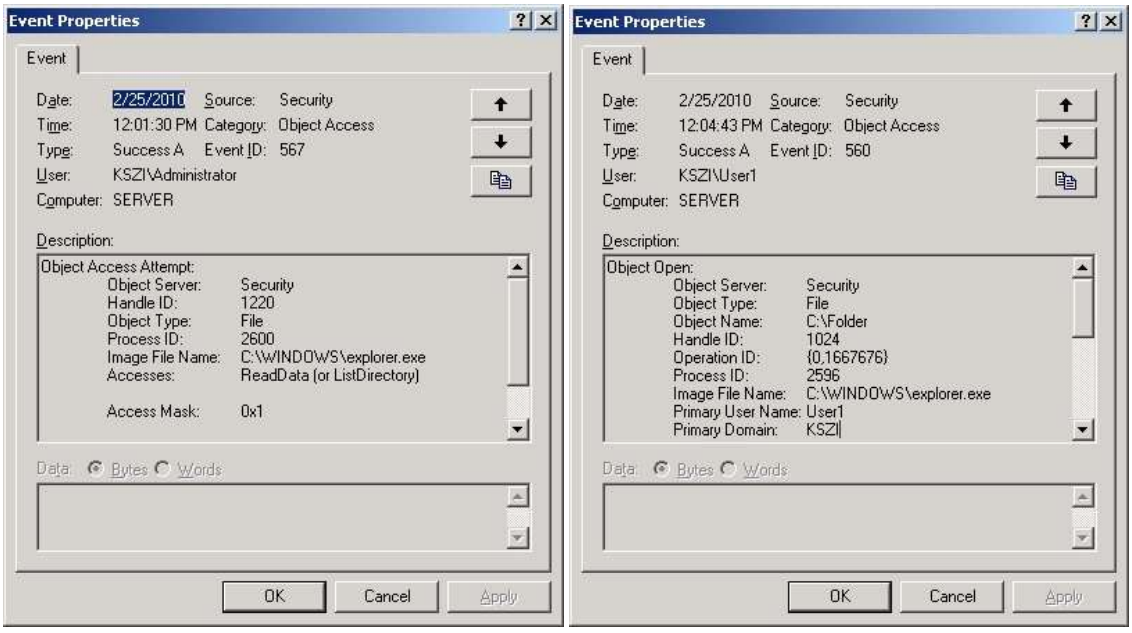

Рис.3.54