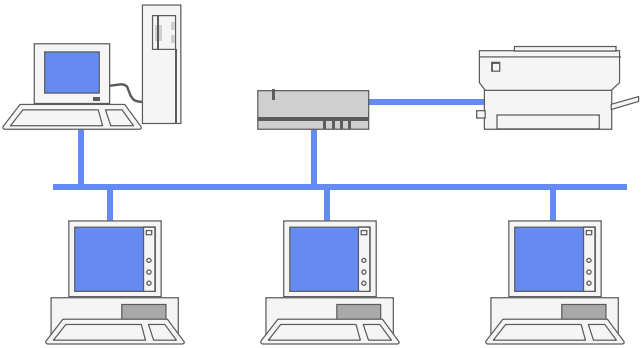
Міністерство освіти України
Львівський державний університет імені Івана Франка

В.М.Горлач, В.М.Макар

Побудова та адміністрування INTRANET-мереж

Частина 2. Адміністрування мереж Windows NT

Тексти лекцій



Рекомендовано до друку
науково-методичною радою
факультету прикладної математики та інформатики.
Протокол № 2 від 13.05.99р.
Методичні матеріали ТЛ № 4/99

Львів ЛДУ 1999

Горлач В.М., Макар В.М. Побудова та адміністрування INTRANET-мереж: Ч. 2. Адміністрування мереж Windows NT: Тексти лекцій.-Львів: Видавничий центр Львів. ун-ту, 1999.- 41 с.

В текстах лекцій розглянуто основні властивості та архітектуру мережної операційної системи Microsoft Windows NT. Висвітлені питання захисту інформації та системи безпеки, використання особливостей файлової системи NTFS, планування моделі мережі, адміністрування облікових записів та ведення системної політики. Описані основні команди режиму командної стрічки та використання командних файлів в адміністративних цілях.

Матеріал цього посібника також може бути корисним адміністраторам корпоративних мереж.

Рецензенти: Р.Є. Рикалюк, канд. фіз.-мат. наук, директор інформаційно-обчислювального центру Львівського державного університету імені Івана Франка;

Ю.В. Нікольський, канд. фіз.-мат. наук, доцент державного університету "Львівська політехніка"

Редактор М.В.Ріпей

Зміст

Лекція 1. Основні властивості та архітектура Windows NT

Універсальна операційна система (ОС) Windows NT уперше з'явилася у продажу в липні 1993 року. Високі вимоги до ресурсів апаратного забезпечення обмежували її використання. Із виходом версії 3.5, в якій значно знизився рівень цих вимог і введено ряд нових функцій, почалося значне збільшення популярності Windows NT. Введення нового інтерфейсу та нових корисних властивостей у версії 4.0 привело до широкого впровадження цієї системи на персональних робочих місцях.

ОС Windows NT складається з двох різних продуктів: Windows NT Server і Windows NT Workstation, кожен з яких здатен функціонувати в мережі як клієнт, так і сервер. Обидва варіанти Windows NT є 32-розрядними ОС з такими спільними властивостями:

- *пріоритетна багатозадачність і багатопотокові обчислення:* компонента ОС Windows NT, яка називається **планувальник задач** (Task Sheduler), регулює виконання процесів центральним процесором або відповідно встановленого графіка, або на основі деякої високопріоритетної події, наприклад переривання. Найбільший пріоритет мають операції введення-виведення, які виконуються в режимі реального часу. Причому виконання цих операцій, які утворюють **активний процес** (foreground process), відбувається одночасно з іншими операціями, які утворюють **фоновий процес** (background process). Більше того, один процес може породити декілька **потоків**, що дає змогу організовувати та проводити багатопотокові обчислення;
- *вбудована мережна підтримка:* на відміну від більшості інших ОС, система Windows NT з самого початку проектувалася для роботи в мережі. Це означає, що мережні засоби Windows NT (зокрема, функції спільного використання файлів, пристроїв та об'єктів) не є надбудовою над ситемою, а її складовою частиною. Windows NT може використовуватись у мережах масштабу великих підприємств, надаючи адміністраторам засоби централізованого управління та контролю корпоративної мережі;
- *підтримка симетричної багатопроцесорної обробки:* Windows NT може працювати в багатопроцесорних системах (у стандартній версії підтримується до 4, а максимальна кількість - 32 процесори). Основу виконавчої системи Windows NT становить **мікроядро**, яке складається з мінімально необхідної кількості сервісних програм і, завдяки цьому, має невеликий розмір. Windows NT підтримує симетричну багатопроцесорну обробку задач, оскільки на кожному процесорі виконується один екземпляр мікроядра;
- *підтримка широкого спектра комп'ютерних платформ:* ОС Windows NT розрахована на незалежність від конкретних апаратних засобів. Windows NT однаково добре працює як на комп'ютерах з Intel-сумісними процесорами типу 386, 486, Pentium, так і на RISC-процесорних системах на базі процесорів типу PowerPC, MIPS R4000, DEC Alpha;

♦ *можливість виконання програм, написаних для інших ОС:* більшість програм, написаних для MS-DOS, Win16, Win32, OS2 і POSIX, без проблем запускаються під управлінням Windows NT;

♦ *підтримка декількох файлових систем:* Windows NT підтримує три файлові системи: стандартну для DOS систему FAT, Windows NT File System (NTFS) і файлову систему CD-ROM (CDFS), яка дає змогу працювати з CD-ROM без драйвера MSCDX. Надійна NTFS дає змогу вживати довгі імена та розрахована на використання влаштованих у Windows NT засобів безпеки та захисту даних;

♦ *захищеність:* Windows NT сертифікована на рівень захисту С2. Це означає, що Windows NT орієнтована на роботу з конфіденційною інформацією. В основі системи захисту Windows NT є об'єктна модель. Кожен ресурс системи має свій об'єкт захисту, який містить інформацію про те, що можна, а що забороняється робити з цим ресурсом;

♦ *надійність:* програми під Windows NT виконуються в окремих адресних просторах. Аварійне завершення однієї з програм не впливає на роботу інших. Крім того, специфічні властивості архітектури Windows NT захищають ОС від програм, які роблять спроби зайняти занадто багато процесорного часу чи використати адресний простір самої ОС.

Між версіями Windows NT Server і Windows NT Workstation є деякі відмінності. Windows NT Workstation може виконувати функції невиділеного серверу в одноранговій мережі, однак використовувати її як повноцінний сервер не можна. Це пов'язано з відсутністю у Windows NT Workstation засобів адміністрування та керування доменом, оптимізації підсистем для виконання сервер-орієнтованих програм типу SQL Server, SNA Server тощо. Окрім того, кількість одночасних під'єднань для Windows NT Server обмежена кількістю придбаних клієнтських ліцензій, тоді як для Windows NT Workstation вона не може бути більшою ніж 10.

Широко відомі ОС DOS, NetWare, Windows 95 жорстко прив’язані до архітектури комп’ютера, не забезпечують достатнього рівня захисту даних і, в основному, зорієнтовані на настільні системи або ж локальні мережі масштабу підрозділу підприємства чи організації.

У системі Windows NT реалізована архітектура клієнт/сервер, в якій прикладні програми не мають прямого доступу до апаратних засобів та захищених компонентів ОС. Усі операції доступу від імені прикладних програм здійснює виконавча система Windows NT - NT Executive.

Будь-яка ОС має ядро, яке постійно знаходиться в оперативній пам’яті і забезпечує виконання мінімального набору системних функцій. Наприклад, у DOS основними компонентами ядра є базова система введення-виведення BIOS (у MS-DOS реалізована файлом IO.SYS), базова система роботи з дисками BDOS та ще ряд функцій, що зв’язують ці компоненти. Всі інші компоненти ОС зберігаються на диску та завантажуються в оперативну пам'ять за потребою.

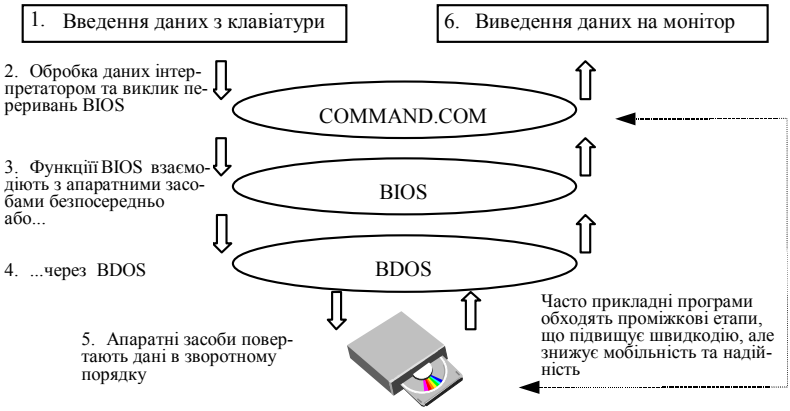


Рис. 1.1. Схема функціонування класичної ОС

На рис. 1.1 зображено роботу DOS: введення команди з клавіатури активізує інтерпретатор команд COMMAND.COM, який аналізує команду та викликає необхідні функції BIOS. Функції BIOS звертаються до дисків не безпосередньо, а використовуючи відповідні функції BDOS. Оскільки функції BIOS та BDOS викликаються майже всіма програмами DOS, вони зберігаються в оперативній пам’яті постійно і становлять, таким чином, частину ядра DOS. Стандартизація апаратної структури персонального комп'ютера дала змогу програмістам, задля збільшення продуктивності, звертатись до низькорівневих апаратних засобів, оминаючи BIOS.

В ОС Windows NT ні еквівалент BIOS – HAL.DLL (Hardware Abstraction Layer – Рівень апаратних абстракцій), що є динамічно завантажуваною бібліотекою, ні еквівалент BDOS (одна з можливих файлових систем) частинами ядра не являються, хоча й виконуються в привілейованому режимі як складові NT Executive. В основі NT Executive є мікроядро, яке складається тільки з тих сервісних програм, постійна наявність яких в оперативній пам’яті є абсолютно необхідною, що забезпечує його мінімальний розмір. Мікроядро керує потоками інформації між різними компонентами системи. Усі запити прикладних програм передаються через мікроядро, яке встановивши достовірність, передає їх від імені підсистеми, в якій були сформульовані ці запити. Така схема взаємодії, яка зображена на рис.1.2, є основою архітектури клієнт/сервер: будь-яка підсистема, яка "обслуговує" інші підсистеми, називається сервером, а будь-яка програма, яка запрошує ці послуги, називається клієнтом. Усі функції Windows NT обробляються за допомогою серверних процесів. Взаємодією клієнтів і серверів керує мікроядро.

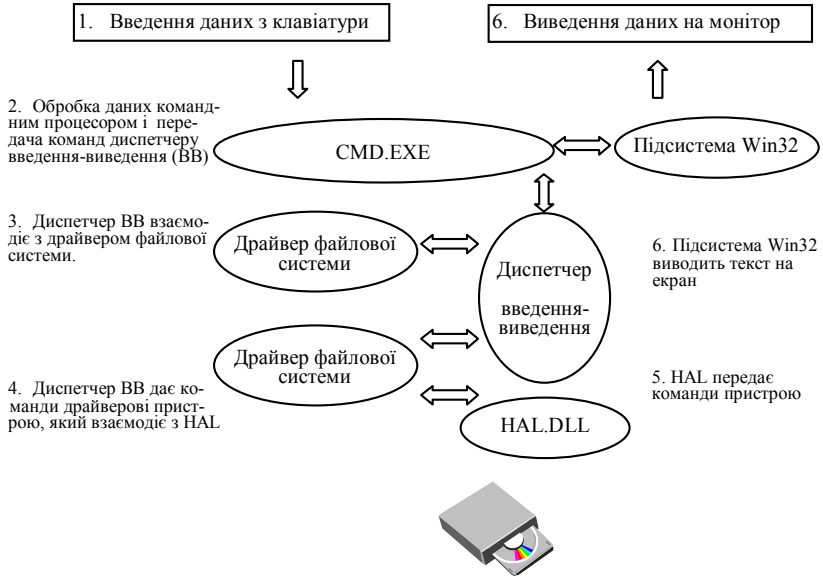


Рис. 1.2. Принцип роботи мікроядра Windows NT

Спільне з Windows 95 (зокрема інтерфейс користувача) значно полегшує процес освоєння Windows NT. Тому у текстах лекцій розглядаємо лише ті властивості цієї потужної та універсальної ОС, які необхідні для побудови та ефективного адміністрування мереж на базі Windows NT.

Лекція 2. Мережні моделі: робочі групи та домени

У мережах, базованих на Windows NT, використовуються дві моделі: *модель робочих груп (workgroup)* та *доменна (domain) модель*.

2.1. Модель робочих груп

Робоча група являє собою набір згрупованих за певним принципом (безпосередня близькість розташування, приналежність до одного підрозділу, спільність задач) комп'ютерів. Робочі групи в мережах з NT-серверами (Windows NT Server) та NT-робочими станціями (Windows NT Workstation) відповідають робочим групам у мережах з ОС Windows for Workgroups та Windows 95. Групування комп'ютерів у робочі групи дає змогу користувачу в своїй групі швидше здійснювати доступ до розподілених для спільного використання ресурсів. Незалежно від загальної кількості вузлів у мережі, комп'ютери однієї робочої групи візуально зібрано на екрані в одному місці, а комп'ютери групи, до якої належить вузол відображаються одразу після виклику *Networks Neibourhoods* (Сетевое окружение).

Адміністрування NT-комп'ютерів у робочих групах аналогічне до адміністрування одного комп'ютера. У кожного NT-комп'ютера своя база облікових записів користувачів SAM (Security Account Manager) і своя політика захисту (Policies). Усі адміністративні дії стосуються тільки одного комп'ютера. Якщо користувачеві потрібен доступ до кількох NT-комп'ютерів, на кожному з них повинен бути створений для нього обліковий запис. На відміну від ОС DOS, Windows for Workgroups, Windows 95, OS/2, процедури реєстрації та контролю доступу до комп'ютера в Windows NT є вбудованими. Використання файлової системи NTFS блокує доступ до даних навіть у випадку завантаження іншої ОС (DOS, Windows 95) з дискети. Отже, доцільність інсталяції Windows NT на один або декілька комп'ютерів, навіть у невеликих мережах, може зумовлюватись необхідністю додаткового захисту доступу до даних, окремих мережних ресурсів або сервісів.

2.2. Доменна модель

Збільшення кількості комп'ютерів та користувачів у робочій групі, з огляду на децентралізацію облікових записів та політику захисту, призводить до неможливості адміністрування та управління мережею у межах моделі робочої групи. Для забезпечення надійного захисту та спрощення управління мережею ОС Windows NT Server пропонує доменну модель. Доменом називають групу комп'ютерів, що використовують *спільну базу облікових записів* та керуються *єдиною політикою захисту*. Централізація цих засобів дає змогу адміністратору ефективно здійснювати управління та захист мережі на рівні підрозділів та підприємства уцілому.

Кожен домен має унікальне ім'я (використання кириличних назв не дозволяється навіть для локалізованих версій ОС) і, в кампусних мережах,

домен ззовні нічим не відрізняється від робочої групи. Однак доступ до ресурсів домену незареєстрованим у домені користувачам заборонений. Незалежно від кількості комп'ютерів у домені, кожен користувач має лише один обліковий запис. NT-сервер (тобто комп'ютер з ОС Windows NT Server), на якому зберігається база облікових записів усього домену, називається *первинним контролером домену* (PDC –Primary Domain Controller). Для забезпечення надійного зберігання такої важливої інформації та підвищення швидкості аутентифікації користувачів у великих мережах база облікових записів SAM автоматично (кожних 5 хвилин) копіюється на інші NT-сервери – *резервні контролери домену* (BDC – Backup Domain Controller). Наявність BDC у домені не є необхідною, однак вельми бажаною. Доступ до ресурсів мережі без процедури реєстрації у домені неможливий, тому контролери домену повинні працювати в режимі non-stop (не вимикатись цілодобово) або ж умикатись першими і вимикатись останніми. У мережах з конфіденційною інформацією контролери домену захищають апаратно (корпуси, жорсткі диски, клавіатура із замками тощо) або фізично, встановлюючи їх у приміщеннях з обмеженим доступом.

Окрім контролерів (PDC та BDC), до складу домену може входити довільна кількість інших NT-серверів (Standalone Server): файл-сервери, принт-сервери, Internet-сервери, сервери застосувань та ін.

У кожному домені може бути лише один первинний контролер. Усі зміни в базі SAM виконуються лише на ньому. BDC забезпечують доступ до бази SAM тільки в режимі читання. Якщо є потреба замінити PDC одним з BDC використовують програму *Server Manager*. Для цього у діалоговому вікні вибирають потрібний BDC-сервер і виконують команду *Promote to Primary*. При цьому статус попереднього PDC автома-тично понижується до BDC. Часто в якості PDC використовують ненайпотужніший з серверів мережі, на якому, однак, не виконуються більше ніякі функції та сервіси. У базі SAM зберігаються облікові записи не тільки користувачів, але й комп'ютерів, а також стандартних та створених груп користувачів. Чим більше записів у базі, тим довше відбувається реєстрація (необхідність завантаження в пам'ять та обробки бази). Рекомендований максимальний розмір бази SAM становить 40 Mb і дає змогу зберігати 40000 облікових записів користувачів, однак обсяг оперативної пам'яті контролера домену повинен у 2,5 раза перевищувати обсяг бази SAM (обчислюючи розмір бази, слід брати до уваги, що запис користувача займає 1 Kb, запис комп'ютера – 0,5 Kb, запис групи користувачів – 4 Kb). Окрім того, якщо база SAM збільшується на кожних дві тисячі записів, рекомендовано додавати в домен один резервний контролер.

2.3. Довірчі відносини

У мережах з кількома доменами реалізацію функцій захисту та адміністрування полегшує налагодження *довірчих відносин* (trust relation-

ships) між доменами. В довірчих відносинах беруть участь домен, що довіряє (trusting domain), та домен, якому довіряють (trusted domain). Домен, що довіряє, розпізнає облікові записи користувачів та їх груп з домену, якому довіряє. Ці облікові записи можуть бути згруповані в локальних групах домену, що довіряє. Довірчі відносини дають змогу користувачам одного домену звертатись до ресурсів іншого домену без додаткової реєстрації. Окрім цього, адміністрування розгалуженої мережі спрощується до управління однією базою SAM та невеликою кількістю локальних груп з одного вузла. Домен, у якому розміщені облікові записи всіх користувачів називається *доменом облікових записів* (account domain).

Довірчі відносини можуть бути одно- та двосторонніми (one- and two-way trust). Будь-який домен може ініціювати налагодження довірчих відносин командою *Trust Relationships* з меню *Policies* програми *User Manager for Domains*, однак завершити їх налагодження можна лише після реалізації таких відносин в обох доменах.

Наявність довірчих відносин між доменами дає змогу користувачу реєструватись з будь-якого вузла мережі. Вказуючи своє ім’я та домен, до якого він відноситься, користувач отримує всі права та привілеї, що надані йому в “рідному” домені. Кожен домен може налагоджувати довірчі відносини одразу з кількома іншими доменами. Залежно від розміру мережі, кількості користувачів та організаційної структури підприємства можна будувати різні доменні моделі: *однодоменну модель, модель з одним майстер-доменом* (майстер-домен являє собою одночасно і trusted domain, і account domain, а всі інші домени нагоджують з ним односторонні довірчі відносини)*, модель з кількома майстер-доменами* (кожний майстер-домен пов'язаний з іншими двосторонніми довірчими відносинами, що дає змогу збільшити кількість користувачів до 40000 і більше) та *модель повністю довірчих відносин* (модель повністю децентралізованого між адміністраторами доменів управління).

Лекція 3. Захист інформації та система безпеки Windows NT

3.1. Рівень захисту С2

Захищена мережна система повинна відповідати певним вимогам. Перелік цих вимог може визначатись кожною організацією чи підприємством. В Україні, наприклад, немає єдиних стандартів: вимоги щодо надійності та безпеки комп’ютерних систем органів державного управління, національної банківської системи, спеціальних служб суттєво різняться між собою. У США базовим рівнем захисту вважаються рекомендації Міністерства оборони на відповідність рівню С2.

Основні положення рівня захисту С2 такі:

- Власник ресурсу (наприклад файла) повинен мати змогу контролювати доступ до нього.
- Операційна система повинна захищати дані, що знаходяться в оперативній пам’яті комп’ютера і належать одному процесові, від викорис-

тання їх іншими процесами. (Windows NT Server захищає ділянку пам'яті, зайняту процесом так, що її вміст не може бути зчитаний навіть після звільнення цієї ділянки. Якщо вилучити файл з диска, користувач не може отримати доступ до даних звільненого дискового простору, навіть якщо цей простір виділяється для запису нового файла).

- Кожен користувач повинен мати індивідуальну ідентифікацію в системі, а система – змогу використовувати цю ідентифікацію для вистежування всіх дій користувача.
- Адміністратори системи повинні мати змогу аудиту (контролю) усіх подій, пов'язаних із захистом системи, а також дій окремих користувачів. Доступ до даних аудиту має бути обмеженим.
- Система повинна захищати себе від втручання типу модифікації працюючої системи або файлів, що зберігаються на диску.

Насправді, розробляючи Windows NT Server, фірма Microsoft пішла у розв'язанні реальних проблем захисту систем набагато дальше від вимог рівня С2. Річ у тім, що багато "реальних" проблем захисту не описані у вимогах стандартів. До таких можна, зокрема, віднести питання, пов'язані із захистом системи при віддаленому доступі. Мережна реєстрація, маршрутизація, передача файлів, електронна пошта, зв'язок з Internet –ці проблеми розв'язує системний адміністратор.

3.2. Модель безпеки Windows NT

На відміну від багатьох інших ОС, засоби захисту в Windows NT не є надбудовою чи окремою підсистемою, а від самого початку проектувались як частина специфікацій на розробку системи.

Основні елементи підсистеми захисту:

- розпорядник локальної безпеки LSA (Local Security Authority);
- менеджер захисту облікових записів SAM (Security Account Manager);
- довідковий монітор захисту SRM (Security Reference Monitor).

Додаткові елементи захисту Windows NT:

- процес реєстрації;
- елементи управління персональним доступом;
- маркери доступу;
- списки контролю доступу ACL (Access Control List).

3.3. Розпорядник локальної безпеки LSA

Підсистема LSA є стрижнем системи захисту Windows NT Server. У її функції входить:

- надання користувачам доступу в систему;
- створення маркерів доступу в процесі реєстрації;
- управління інтерактивним процесом аутентифікації користувача;
- управління локальною політикою захисту;
- контроль політики аудиту;
- запис повідомлень аудиту, що надходять від довідкового монітора захисту SRM, у журнал подій.

3.4. Менеджер захисту облікових записів SAM

Підсистема SAM забезпечує роботу з однойменною базою даних захисту облікових записів, у якій зберігається інформація про всі облікові записи користувачів, груп і комп'ютерів. Менеджер SAM відповідає за звірку інформації, що вводиться користувачем під час реєстрації з тією, що зберігається в базі захисту, а також за надання користувачеві його ідентифікаційного коду SID (*Security ID*), а також SID тих груп, до яких користувач належить. Вилучення користувача з бази SAM приводить до вилучення його SID. Новий обліковий запис, навіть з тим самим ім'ям та паролем, отримує новий SID, тому інформація про права та привілеї цього користувача не може бути таким чином відновлена.

Залежно від конфігурації мережі, доступ до мережних ресурсів здійснюється з використанням бази SAM:

- у моделі робочих груп – розміщеної на комп'ютері, якому належить ресурс;
- у доменній моделі – контролера домену.

3.5. Довідковий монітор безпеки SRM

Підсистема SRM забезпечує захист ресурсів та об'єктів від неавторизованого доступу та модифікації. Безпосередній доступ до об'єкта в Windows NT заборонений – усі запити користувачів перевіряються монітором SRM. Наприклад, коли відкривається на редагування файл, SRM перевіряє дескриптор захисту файла з інформацією, що міститься в маркері доступу користувача, і після цього робить висновки щодо можливості надання доступу до файла. Дескриптор захисту містить усі входи контролю доступу ACE (Access Control Entries), які й складають список контролю доступу ACL файла. ACE визначає доступ до об'єкта на основі ідентифікаторів захисту та особливих привілеїв доступу, які містяться в ньому. ACE додаються до ACL під час визначення користувачем персонального доступу до створеного ним об'єкта. Якщо власник об'єкта не встановив персонального доступу до об'єкта, то створюється ACL за замовчуванням. Файл, що не має свого ACL, відкритий для всіх видів доступу.

Довідковий монітор безпеки перевіряє всі ACE в ACL визначаючи для користувача конкретний тип доступу: його персональний SID або SID однієї з груп, до яких належить користувач, порівнюється зі списком ACE, а вид дії - із можливостями доступу, які описані в ACE. У випадку збігу користувачеві надається доступ. При цьому подальші перевірки не проводяться, а доступ здійснюється на підставі створеного відповідного вказівника на файл.

ACE сортуються за типом доступу - надати чи заборонити. У Windows NT заборона доступу завжди має вищий пріоритет, ніж дозвіл доступу, тобто спочатку перевіряються ACE з відмовою в доступі, а потім - з дозволом доступу. Це означає, що якщо хоча б одній з груп, до яких належить користувач, доступ заборонено, то, незалежно від того, чи має цей користувач персональний доступ, йому буде відмовлено в доступі. Отже,

якщо групі ***Everyone*** заборонено доступ до об'єкта, то для всіх користувачів, зокрема і власника об'єкта, доступ буде заборонено. Однак заборона доступу до об'єкта не означає заборону власникові цього об'єкта змінити вид доступу.

3.6. Процес реєстрації

Процес розпочинається з діалогового вікна з пропозицією натиснути комбінацію клавіш Ctrl+Alt+Del (перед цим вікном можна вивести попередження про легальність використання). Такий початок процесу реєстрації має за мету надійно захистити від програм, які виконуються у фоновому режимі та мають за мету "підглянути" реєстраційні дані користувача. Після цього з'являється діалогове вікно процесу *WinLogon* (див. рис.3.1).

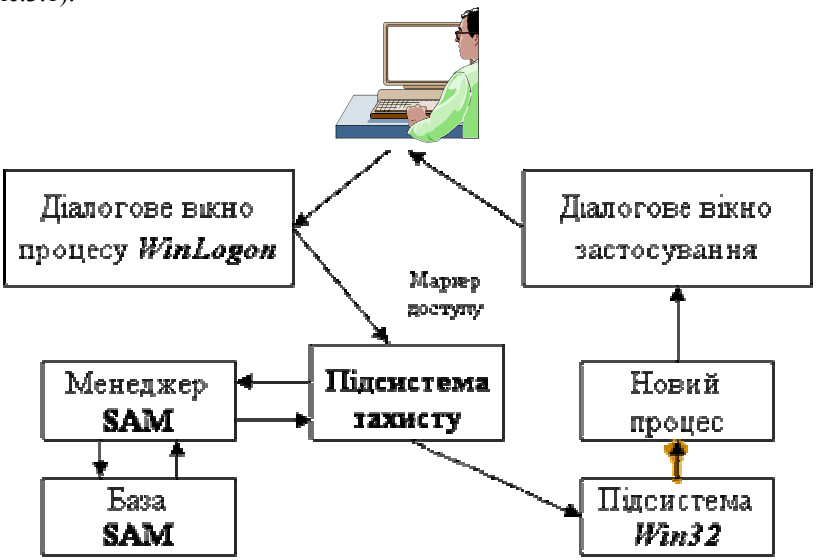


Рис. 3.1. Процес реєстрації в Windows NT

У цьому вікні користувач уводить своє ім'я, пароль та ім'я серверу або домену, до якого йому необхідно отримати доступ. Якщо ж сервер або контролер домену недоступні у випадку збою мережі (або, що ще гірше, вимкнуті), користувач буде зареєстрований локально з використанням інформації в базі SAM своєї робочої станції. Наступний етап – аутентифікація користувача. Інформація, введена в діалоговому вікні, обробляється менеджером захисту облікових записів SAM та порівнюється з інформацією в базі SAM контролера домену. Якщо дані збігаються, контролер посилає на робочу станцію підтвердження доступу та додаткову інформацію про користувача. Розпорядник локальної безпеки LSA створює об'єкт – *маркер доступу*, який можна назвати "посвідкою особи". Маркер доступу містить SID та ім'я користувача і груп, до яких він належить.

Зв'язок процес-маркер називають *суб'єктом*. Суб'єкти оперують над об'єктами Windows NT за допомогою системних сервісів. Створений маркер доступу передається процесу WinLogon, який передає управління та маркер підсистемі Win32.

Ще одна корисна можливість Windows NT - це автоматична реєстрація. Вхід у систему здійснюється з використанням заздалегідь визначеного спеціального облікового запису. Перемкнутися на автоматичну реєстрацію можна за допомогою утиліти *AutoLogon*.

Лекція 4. Адміністрування облікових записів

4.1. Багаторівнева адміністративна модель

Обліковим записом (ОЗ) називається сукупність прав, які має конкретний користувач. *Групою* називається набір прав на доступ до ресурсів, який присвоюється одразу декільком користувачам. Групи дають змогу адміністраторові розглядати облікові записи великої кількості користувачів як один запис, що суттєво спрощує проблеми адміністрування. Делегуючи обліковим записам груп ті чи інші адміністративні функції, адміністратор має змогу побудувати багаторівневу модель управління ресурсами мережі.

Для реалізації такої адміністративної моделі в Windows NT використовуються три типи облікових записів:

1. *Облікові записи користувачів* (*локальні* – на комп'ютері, або *глобальні* – в домені). У кожного користувача в системі є свій, захищений паролем, обліковий запис.
2. *Локальні групи.* Локальні групи визначаються на кожній машині. У них можуть входити облікові записи користувачів та глобальні групи.
3. *Глобальні групи.* Глобальні групи визначаються на рівні домену.

4.2. Облікові записи користувачів

Кожен користувач має своє *ім'я (User name)* та *пароль*. В одному домені або робочій групі не може бути декілька користувачів з одним іменем. У різних доменах імена можуть збігатися, оскільки повне ім'я користувача складається з двох компонентів: *Ім'я Домену\ Ім'я Користувача*. Під час визначення нового користувача в системі створюється ідентифікаційний код SID, за допомогою якого система надалі розпізнаватиме цього користувача. Саме цей унікальний код, а не ім'я користувача використовується для доступу до ресурсів. Саме тому, якщо знищити старий ОЗ і після цього створити новий з тим самим іменем, новостворений користувач не буде мати прав та привілеїв "старого" користувача з тим же іменем.

ОЗ користувачів Windows NT можуть бути *локальними* або *глобальними*. Локальні записи визначають права на конкретному комп'ютері, які не розповсюджуються на ресурси домену. Для отримання доступу до ресурсів домену користувач повинен зареєструватися в домені, використовуючи свій глобальний ОЗ. У цьому випадку аутентифікація відбувається не на тому комп'ютері, з якого користувач вводить пароль та ім'я, а на

PDC (або на одному з BDC) домену. Якщо користувач здійснює доступ до ресурсу, який знаходиться в домені, з яким не налагоджені довірчі відносини, і в якому немає його глобального запису, то на сервері, що містить необхідний ресурс, повинен бути локальний ОЗ цього користувача. У табл. 4.1 наведено використання глобальних та локальних ОЗ.

Табл. 4.1. Використання глобальних та локальних ОЗ

Домен А	Домен В	Довірчі відносини	Пояснення
○	x	x	Користувач, що має локальний ОЗ на одному з серверів домену А, має доступ лише до ресурсів цього серверу.
●	x	x	Користувач з глобальним ОЗ в домені А позбавлений доступу до ресурсів домену В.
●	○	x	Користувач з глобальним ОЗ в домені А і локальним ОЗ на сервері С домену В має вільний доступ до ресурів домену А і доступ до ресурсів серверу С. При цьому вимагається додаткова реєстрація на сервері С.
●	●	x	Користувач з глобальним ОЗ в домені А і глобальним ОЗ в домені В має вільний доступ до ресурів обох доменів. При цьому вимагається додаткова реєстрація в домені В.
●	x	В довіряє А	Користувач з глобальним ОЗ в домені А має право доступу до ресурсів домену В
● - глобальний ОЗ, ○ - локальний ОЗ, x - відсутність ОЗ			

В останньому випадку вищенаведеної таблиці можлива така ситуація: користувач з довільного комп'ютера домену В може зареєструватися (а отже, і отримати доступ) у домені А. Це досягається за допомогою так званої ***наскрізної авторизації***. За допомогою наскрізної авторизації користувач, маючи ОЗ в одному домені, здійснює доступ до ресурсів домену, в якому для нього немає ОЗ. Це забезпечується довірчими відносинами між доменами. Наскрізна авторизація відбувається у двох випадках: у процесі реєстрації в домені, що довіряє (trusting domain), і під час доступу до ресурсів домену, якому довіряють (trusted domain).

Після інсталяції Windows NT Server у системі створюється два ОЗ:

- *Administrator* (у російській версії - *Администратор*) з паролем, заданим під час інсталяції, та майже необмеженими правами,
- *Guest* (*Гость*) з максимально обмеженими правами, але можливістю увійти в систему без пароля.

Ці ОЗ називаються вбудованими (build-in). Рекомендується створити новий ОЗ з адміністративними правами, а вбудовані заблокувати. Для створення нових ОЗ, а також для їх редагування та знищення, використовують програму *User Manager* (для NT Workstation) і *User Manager for Domain* (для NT Server). Для початкуючих адміністраторів створення нових ОЗ полегшується майстром *Add User Account Wizard*. За допомогою *User Manager* можна створити лише локальні ОЗ для тієї робочої станції, на якій вона виконується. Якщо *User Manager* знаходиться на одному з контролерів домену, то можна також створити й глобальний ОЗ у цьому домені, а також у будь-якому іншому домені, що йому довіряє. Причому треба пам'ятати, що під час запуску *User Manager* на BDC для створення

нового ОЗ, PDC повинен бути доступний в мережі, оскільки модифікація бази SAM можлива лише на PDC. Основна відмінність *User Manager for Domain* полягає в тому, що за допомогою цієї програми можна вибирати домен, у якому буде створюватися чи модифікуватися ОЗ (попередньо зареєструвавшись у цьому домені як адміністратор). Крім того, можна також задати період часу, коли користувачі можуть реєструватися, комп'ютери, на яких вони можуть це зробити, термін дії ОЗ тощо. Обидві версії *User Manager* запускаються за допомогою однойменних команд у підменю *Administrative Tools* меню *Programs* стартового меню. Спільними, для обох версій *User Manager*, параметрами, які можна визначити у процесі створення нового ОЗ є:

- пароль,
- правила зміни пароля користувачем,
- локальні групи, в які входить користувач,
- профіль користувача.

Пароль є необхідним для входу в систему Windows NT. Він може складатися не більше ніж з 14 символів, при цьому враховується також регістр. Такі параметри пароля, як термін його дії, мінімальна довжина та інші визначаються політикою захисту паролів. Пароль, а також правила зміни пароля, визначаються адміністратором під час створення нового ОЗ. Після зміни пароля користувачем адміністратор вже не може його взнати. У табл. 4.2 наведені передбачені в Windows NT правила зміни пароля.

Табл. 4.2. Правила зміни пароля в Windows NT

Правило	Пояснення дії правила
Users Must Change Password at Next Logon	Змушує користувача змінити пароль під час першої реєстрації в системі. Задається за замовчуванням під час створення нового ОЗ
User Cannot Change Password	Забороняє змінювати пароль. Застосовується для ОЗ з обмеженим доступом до ресурсів
Password Never Expires	Термін дії пароля необмежений. Має перевагу над параметром Maximum Password Age політики захисту ОЗ і над правилом Users Must Change Password at Next Logon
Account Disabled	Призупиняє можливість застосування цього ОЗ. Блокування ОЗ, на відміну від знищення, не скасовує прав і привілеїв цього ОЗ

4.3. Локальні групи

На NT-машинах, що не уведені в домен, створюються і підтримуються тільки локальні групи. Локальна група надає права та доступ тільки для тієї системи, в якій вона визначена. Якщо система є частиною домену, то в локальну групу можуть входити ОЗ користувачів та глобальні групи домену, в якому знаходиться ця локальна група, а також ОЗ користувачів та глобальні групи доменів, з якими налагоджено довірчі відносини. Важливе призначення локальних груп - об'єднання в одне ціле декількох глобальних груп з різних доменів. Замість того, щоб присвоювати права кожній з глобальних груп, достатньо створити одну локальну групу, присвоїти їй потрібні права та увести до неї глобальні групи. Членство в локальній групі дає змогу користувачам інших доменів мати доступ до ресурсів цього домену.

Є два рівні локальних груп: *рівень робочої станції* та *рівень домену*. Локальні групи робочої станції використовуються тільки на тій NT-станції, на якій вони створені. Користувач такої локальної групи не має доступу до ресурсів інших комп'ютерів. Локальні групи домену створюються на NT-серверах і їх вплив поширюються на всі NT-сервери (але не на NT-станції) в домені, на які копіюється база SAM. Користувачі локальної групи домену можуть мати доступ лише до ресурсів того домену, в якому визначена ця локальна група. У NT Workstation є такі вбудовані локальні групи: *Administrators, Power Users, Users, Guests, Everyone, Backup Operators, Replicator*. Windows NT Server додатково включає *Server Operators, Account Operators, Print Operators*.

4.4. Глобальні групи

Мета створення глобальної групи – зібрати разом користувачів для уведення їх у ту чи іншу локальну групу. Права користувачів глобальної групи визначаються шляхом уведення глобальної групи в локальну, яка має відповідні права. Зокрема, така процедура дає змогу надати користувачам глобальної групи доступ до ресурсів всіх NT-станцій за допомогою однієї операції. Глобальна група містить облікові записи користувачів домену, але не може містити в собі інші локальні або глобальні групи. Новостворений ОЗ користувача автоматично уводиться в глобальну групу *Domain Users.* Крім цієї групи, в Windows NT Server є такі вбудовані глобальні групи: *Domains Admin* та *Domain Guests*. Група Domains Admins входить в локальні групи *Administrators* домену та кожної NT-станції домену. В групу *Domain Users* входять ОЗ усіх користувачів домену, зокрема і вбудовані ОЗ.

Створюються нові (модифікуються існуючі) локальні та глобальні групи з допомогою команд *New Local Group* та *New Global Group* (*Group Properties*) утиліти *User Manager* (*User Manager for Domain*). Керування групами здійснюється за допомогою діалогових вікон *Group Properties* і *User Properties*. Ці діалогові вікна викликаються шляхом вибору команди *Properties* меню *User* після вибору конкретного користувача (групи) в головному вікні програми *User Manager* (*User Manager for Domain*). У *Group Properties* робота ведеться зі списком користувачів тієї чи іншої групи. А в діалоговому вікні *User Properties* для кожного користувача визначаються групи, до яких він належить.

Операційна система додатково створює *спеціальні групи*, серед яких найчастіше вживається група *Everyone* (*Все*) – яка об'єднує всіх, хто працює на комп'ютері, зокрема і спеціальну групу *SYSTEM* самої ОС.

4.5. Права та привілеї груп

Привілей – це надання користувачеві змоги виконати певну дію в системі. Привілеї застосовуються до системи у цілому. *Права* – це правила, пов'язані з певним об'єктом (наприклад файлом, каталогом, принтером тощо). Привілеї мають пріоритет перед правами: якщо користувач не має прав доступу до ресурсу, але група, до якої він належить, має привілеї доступу до всіх ресурсів системи, то він може здійснити доступ до цього ресурсу.

Привілеї визначаються в діалоговому вікні *User Rights Policy (Политика привилегий)* утиліти *User Manager for Domains* (рис.4.1).

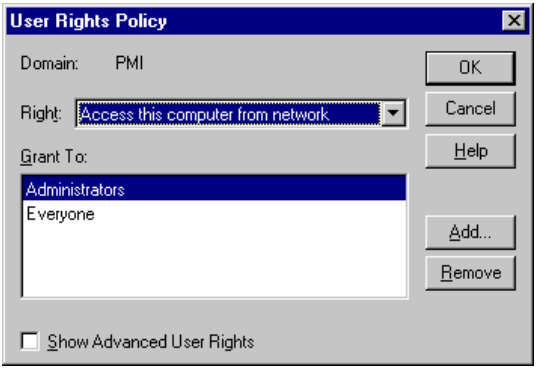


Рис. 4.1. Діалогове вікно *User Rights Policy*

Табл. 4.3. Основні привілеї Windows NT

Привілей	Дає змогу
Access this computer from network	Під'єднуватись до комп'ютера з мережі
Add workstation to domain	Додавати нові робочі станції в домен
Back up files and directories	Виконувати резервне копіювання файлів та каталогів (має пріоритет перед обмеженням прав доступу до файлів та каталогів)
Change the system time	Змінювати системний час на комп'ютері
Load and unloaded device drivers	Завантажувати (вивантажувати) драйвери пристроїв
Log on locally	Реєструватись у системі з клавіатури комп'ютера
Manage auditing and security log	Визначати типи подій, які необхідно реєструвати в журналі подій, переглядати журнал, вилучати з нього записи
Restore files and directories	Відновлювати файли та каталоги,має пріоритет перед обмеженням прав доступу до файлів та каталогів
Shut down the system	Вимикати комп'ютер
Take ownership of files and other ...	Вступати в володіння файлами, каталогами тощо

Окрім наведених у таблиці, є ряд додаткових привілеїв, для роботи з якими слід помітити опцію *Show Advanced User Rights* у діалоговому вікні *User Rights Policy*.

Привілеї локальних груп, що визначаються системою за замовчуванням, наведені у таблицях 4.4, 4.5.

Табл. 4.4. Привілеї та основні можливості локальних груп NT- Server

	Administrators	Server Operators	Account Operators	Print Operators	Backup Operators	Console Operators	Replicators	Everyone	Users	Guests
Привілеї										
Реєструватись локально	■	■	■	■	■	■				
Здійснювати доступ з мережі	■					■		■		
Вступати в володіння файлами	■									
Управляти журналом аудиту та захисту	■					■				
Змінювати системний час	■	■				■				
Вимикати систему	■	■	■	■	■					
Виконувати резервне копіювання	■	■			■	■				

Відновлювати файли та каталоги										
Можливості										
Створювати та редагувати облікові записи										
Створювати та редагувати глобальні групи										
Створювати та редагувати локальні групи										
Надавати привілеї користувачам										
Замикати комп'ютер										
Відмикати комп'ютер, замкнутий іншими										
Форматувати жорсткий диск										
Створювати спеціальні групи										
Володіти										

локальним профілем										
Надавати папки в спільне використання										
Надавати принтери в спільне використання										

Табл. 4.5. Привілеї та основні можливості локальних груп NT-Workstation

	Administrators	Power Users	Users	Guests	Everyone	Backup Operators
Привілеї						
Реєструватись локально						
Здійснювати доступ з мережі						
Вступати в володіння файлами						
Управляти журналом аудиту та захисту						
Змінювати системний час						

Вимикати систему						
Вмикати систему з віддаленої станції						
Виконувати резервне копіювання						
Відновлювати файли та каталоги						
Можливості						
Створювати та редагувати облікові записи						
Створювати та редагувати локальні групи						
Надавати привілегії користувачам						
Замикати комп'ютер						
Відмикати комп'ютер, замкнутий іншими						
Форматувати жорсткий диск						
Створювати спільні групи						
Володіти локальним профілем						
Надавати каталоги в спільне використання						
Надавати принтери в спільне використання						

Лекція 5. Системна політика

У попередній лекції, розглядаючи засоби адміністрування індивідуальних ОЗ, наведено можливості визначення правил зміни пароля і привілеїв для кожного користувача. Однак, є ряд спільних для серверу чи домену в цілому параметрів, які дають змогу суттєво підвищити захищеність. Ці параметри об'єднані одним загальним поняттям - ***політика ведення облікових записів.***

5.1. Політика ведення ОЗ

Основним інструментом керування політикою ведення ОЗ у Windows NT є *User Manager* (*User Manager for Domains*). Політикою задаються такі параметри ОЗ, як максимальний термін дії пароля, мінімальна довжина пароля, мінімальний термін збереження пароля незмінним, унікальність пароля, блокування ОЗ у випадках невдалих спроб реєстрації, термін блокування та ін. Задання цих параметрів відбувається в діалоговому вікні *Account Policy* (рис.5.1), яке викликається командою *Account* меню *Policy*.

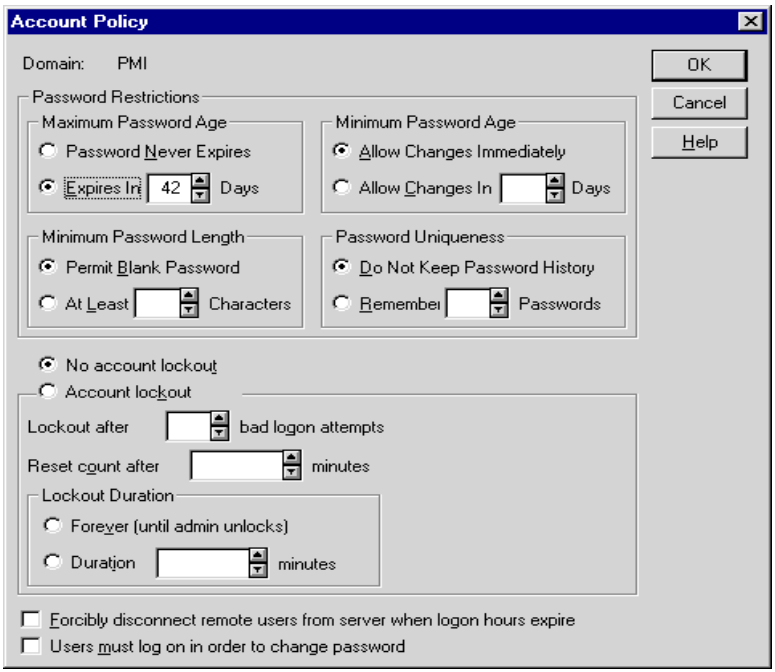


Рис. 5.1. Діалогове вікно *Account Policy*

5.2. Профіль користувача, домашній каталог та сценарій реєстрації

Профілем користувача називається файл, що містить інформацію про користувача: параметри робочого середовища, деякі параметри ОЗ та ін. *Домашній каталог* – це місце збереження персональних файлів користувача, тобто каталог, який за замовчуванням відкривається в діалогових

вікнах *File Open* і *File Save As*. Під *сценарієм реєстрації* розуміють командний файл, який виконується після реєстрації користувача в системі. Профіль користувача пов'язує домашній каталог і сценарій реєстрації з конкретним ОЗ. Це прискорює процес реєстрації користувачів і дає змогу адміністратору контролювати його.

Кожен користувач Windows NT (крім Guest), за замовчуванням, має свій профіль. Профілі поділяються на обов'язкові, персональні та профілі за замовчуванням. Якщо користувачеві назначений *обов'язковий* профіль, то всі його зміни, зроблені користувачем протягом сеансу роботи не зберігаються. Під час наступної реєстрації цього користувача в системі відновлюються параметри обов'язкового профілю. *Персональний* профіль є повною протилежністю обов'язковому профілю. Будь-які зміни будуть збережені та відновлені під час наступного сеансу. Персональні профілі рекомендується зберігати на сервері в загальнодоступному каталозі, що дає змогу користувачеві, зареєстрованому на будь-якій робочій станції, мати своє персональне робоче середовище. *Профіль за замовчуванням* - стандартний профіль Windows NT – застосовується, якщо:

- у користувача немає персонального профілю;
- користувач ще не реєструвався у системі;
- у момент реєстрації відсутній доступ до персонального профілю;
- користувач реєструється як гість.

Змінений профіль за замовчуванням стає персональним профілем, якщо під час наступної реєстрації не буде інших доступних профілів. Якщо в системі ніхто не зареєстрований, то з'являється *системний профіль*. У цей момент на екран виводиться діалогове вікно з запрошенням натиснути комбінацію клавіш Ctrl+Alt+Del.

Профілі автоматично зберігаються в реєстрі. Тому профіль користувача, що реєструється на робочій станції, залежить від того, де він реєструвався раніше. Якщо на цій же робочій станції, то використовується локальний профіль цієї станції. У випадку переходу на іншу робочу станцію використовуватиметься профіль нової станції. Профілі, які зберігаються в реєстрі серверу, називаються серверними профілями. Місцезнаходження серверних профілів задається в базі SAM домену. Серверні профілі використовуються завжди, незалежно від того, де реєструється користувач. Окрім автоматичного збереження в реєстрі, профілі можна зберігати у файлах, присвоївши одне з розширень: **.usr** для персональних і **.man** для обов'язкових. Далі адміністратор вибирає той чи інший файл профілю і призначає його конкретному користувачеві.

Профіль користувача призначається в діалоговому вікні *User Envroment Profile* (рис.5.2), яке викликається за допомогою кнопки *Profile* вікна *User Properties* програми *User Manager*.

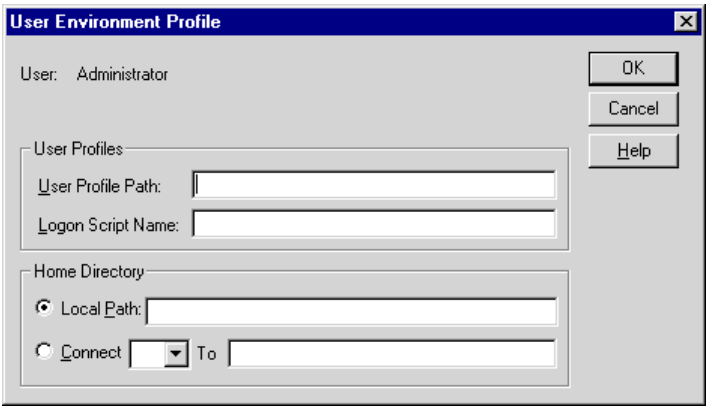


Рис. 5.2. Діалогове вікно *User Enviroment Profile*

У цьому ж вікні задаються домашній каталог та ім'я сценарію реєстрації. За замовчуванням домашній каталог -\USERS\DEFAULT- знаходиться на тому диску, де інстальована ОС. Його можна змінити на інший локальний чи мережний каталог на сервері. Якщо розглядається локальний ОЗ, то рекомендується створювати домашній каталог на робочій станції (поле *Local Path*). Якщо користувач належить до домену, то краще визначити домашній каталог на сервері (відмітити опцію *Connect* і ввести в полі *To* мережне ім'я ресурсу).

У полі *Logon Script Name* можна задати ім'я файла, в якому зберігається сценарій реєстрації. Сценарієм реєстрації може бути командний файл з розширенням **.cmd** або **.bat**, або виконавчий файл. Найчастіше сценарій реєстрації використовується для підключення до мережних пристроїв або запуску певної прикладної програми.

5.3. Редактор системної політики

Починаючи з версії 4.0, у Windows NT для формування профілів використовується програма *System Policy Editor* (*Редактор системної політики*, SPE). За допомогою SPE можна визначати політику для користувачів і комп'ютерів, на яких інстальовано як Windows NT, так і Windows 95. Усі елементи політики щодо користувачів домену поділяються на такі категорії:

- *Control Panel*: Дає змогу обмежити доступ до параметрів дисплея в Control Panel.
- *Desktop*: Визначає оформлення робочого столу.
- *Shell*: Визначає обмеження на елементи інтерфейсу, вміст деяких папок.
- *System*: Визначає обмеження на використання засобів редагування реєстру та запуску програм.
- *Windows NT Shell*: Надає змогу повністю перевизначати вміст папок StartUp, Programs і т.д., а також піктограмок для їх відображення на робочому столі.
- *Windows NT System*: Дає змогу визначати змінні оточення для користувача.

Ці елементи системної політики можна застосовувати для всіх користувачів домену за замовчуванням, для окремих користувачів або груп, а також для локальних користувачів. Детальніше ознайомитись з наведеними вище параметрами можна в [1].

SPE дає змогу також визначати параметри системної політики як для всього домену, так і для окремо взятих комп'ютерів. Визначені за замовчуванням параметри системної політики щодо комп'ютерів використовуються під час реєстрації користувача, до якого не застосовується системна політика. Усі елементи системної політики щодо комп'ютера поділяються на такі категорії:

- *Network*: Визначення правил проведення системної політики.
- *System*: Визначення параметрів, необхідних для здійснення керування за протоколом SNMP, а також вмісту папки StartUp.
- *Windows NT Network*: Визначення обмежень на використання адміністративних каталогів.
- *Windows NT Printers*: Визначення параметрів друку.
- *Windows NT Remote Access*: Визначення параметрів віддаленого доступу.
- *Windows NT User Profiles*: Визначення параметрів профілів користувачів.

SPE працює у двох режимах: *реєстру* і *файла політики*. В першому режимі можна безпосередньо редагувати значення, які зберігаються в реєстрі локального або будь-якого віддаленого комп'ютера. Причому усі зміни відразу набирають чинності. Цей режим роботи вмикається шляхом вибору з меню *File* команди *Open Registry* (для модифікації реєстру локального комп'ютера) або команди *Connect* (для віддаленого комп'ютера). У другому режимі можна створювати або модифікувати файли системної політики. У цьому випадку реєстр редагується опосередковано, а зміни набирають чинності після перереєстрації користувача. Для роботи в цьому режимі в меню *File* слід вибрати команду *Open Policy*.

Незалежно від режиму роботи SPE, об'єкт системної політики (користувач чи комп'ютер) зображається у вигляді значка з відповідним підписом. Для зміни параметрів системної політики треба двічі клацнути лівою кнопкою миші на відповідному значку. Наприклад, щоб модифікувати параметри, визначені за замовчуванням для всіх користувачів (комп'ютерів), треба двічі клацнути на значку *Default User (Default Computer)*. Після цього з'явиться діалогове вікно, в якому буде відображено дерево параметрів системної політики вибраного об'єкта, згрупованих за вищеописаними категоріями.

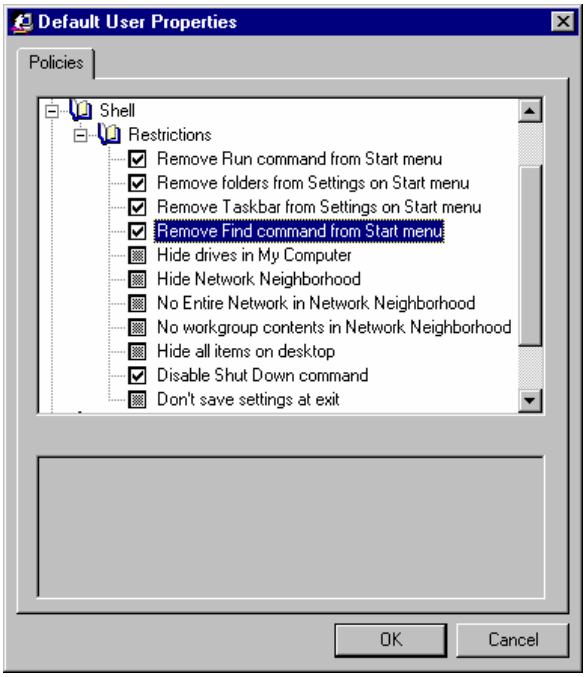


Рис. 5.3. Діалогове вікно SPE категорії *Shell* для *Default User*.

Системна політика може бути завантажена на комп'ютер автоматично або примусово. Для автоматичного завантаження файл системної політики повинен знаходитися на PDC-сервері в каталозі:

\\PDC\netlogon\congif.pol – для клієнтів Windows 95 і

\\PDC\netlogon\ntcongif.pol – для клієнтів Windows NT.

У випадку примусового завантаження треба спочатку вказати параметр *Remote Update*, який знаходиться у гілці *System policies update* категорії *Network* значка, що являє собою певний об'єкт системної політики. Крім того, необхідно в полі *Update mode* вказати тип завантаження *Manual (use specific path)*, а в полі *Path for manual update* - повний шлях до файла системної політики.

Системну політику можна також проводити щодо груп користувачів. При цьому використовуються лише глобальні групи, що визначені в *User Manager for Domains*. Для занесення групи в файл системної політики слід за допомогою команди *Add Group* з меню *Edit* вибрати потрібну групу зі списку, що з'явиться на екрані.

Лекція 6. Файлова система NTFS. Доступ до файлів і каталогів

Будь-яку ОС важко уявити без певної файлової системи, яка є необхідною для роботи із зовнішніми носіями пам'яті, наприклад жорсткими дисками. ОС Windows NT підтримує декілька файлових систем, серед яких найважливішою є, "рідна" для NT, система NTFS (**N**ew **T**echnology **F**ile **S**ystem).

6.1. Загальні властивості та можливості NTFS

NTFS - унікальна файлова система. Вона призначена для використання в комп'ютерних системах від найпростішої робочої станції до серверу класу мейнфрейм. Можливості NTFS дають змогу працювати з дуже великими дисками (до 2^{64} байт). У системі NTFS операції з даними протоколюються, завдяки чому Windows NT швидко відновлює стан файлової системи після аварійного вимкнення. Операції на диску NTFS розглядаються як транзакції і реєструються в спеціальному файлі. Під час завантаження системи драйвер NTFS перевіряє цей файл на наявність незавершених транзакцій, і "вивантажує" їх. Починаючи з версії NT 3.51, файлова система NTFS використовує для роботи з файлами та каталогами атрибут *Compress* (компресія). Засоби NTFS забезпечують майже 50%-не зменшення розміру текстових файлів, 40%-не - виконавчих модулів і ще більший ступінь компресії розріджених файлів, наприклад файлів баз даних. Завдяки використанню комбінації динамічного кешування диска (дані декомпресуються під час передавання в кеш) з асинхронним введенням-виведенням (дає змогу виконувати декомпресію паралельно зі зчитуванням наступного блока даних з диска) компресія майже не впливає на продуктивність Windows NT. І нарешті, NTFS є чи не єдиною файловою системою, яка забезпечує захист інформації: дає змогу контролювати звернення користувачів до файлів, визначати для різних користувачів різні права доступу.

6.2. Структура файлової системи NTFS

Файлова система NTFS розглядає усі файли як об’єкти з атрибутами, визначеними користувачем або системою. Будь-яка інформація на диску NTFS організована у вигляді файла або частини файла. Частиною файла є навіть дані, які описують саму файлову систему. Кожен файл на диску NTFS має свій запис у спеціальному файлі, який називається *головною файловою таблицею* (*Master File Table, MFT*). Перших 16 записів MFT зарезервовані для потреб самої файлової системи NTFS. Перший запис описує безпосередньо головну файлову таблицю. Другим записом є *дзеркальний запис* MFT. Якщо перший запис MFT зруйнований, то NTFS використовує дзеркальний запис для пошуку дзеркального файла MFT, перший запис якого повністю ідентичний до першого запису MFT. Місцезнаходження сегментів даних MFT та дзеркального файла MFT записані в секторі початкового завантаження. Третій запис MFT – файл реєстрації (log file), який використовується для відновлення файлів. Сімнадцятий і наступні записи використовуються файлами та каталогами, які також роз-

глядаються як файли NTFS). На рис.6.1 схематично зображено спрощену структуру MFT.

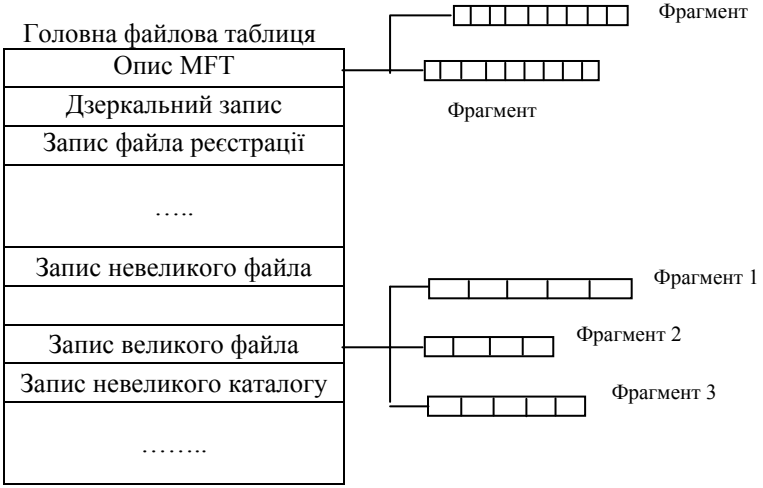


Рис. 6.1. Організація головної файлової таблиці

Для кожного запису MFT відводиться певна кількість дискового простору. Запис MFT для файла (каталогу) складається з набору його атрибутів. Атрибути можуть бути *резидентними* (містяться всередині запису MFT) і *нерезидентними* (знаходяться в іншому місці на диску). Невеликі файли (розміром до 1500 байт) повністю розміщуються всередині запису MFT і, таким чином, усі атрибути такого файла є резидентними. Структура запису MFT для невеликих файлів схематично зображена на рис.6.2.

Стандартна інформація	Ім'я файла	ACL файла	Дані файла або вказівник	

Рис. 6.2. Структура запису MFT для невеликого файла

Деякі атрибути, такі як ім'я файла чи дата створення, завжди є резидентними. Набір атрибутів файлів є розширюваним. Наприклад, у версії 3.51 з'явився новий атрибут Compress. Записи MFT для каталогів, аналогічно до записів для файлів, знаходяться всередині MFT. Записи для каталогів замість даних містять індексну інформацію. Невеликі записи каталогів повністю знаходяться всередині структури MFT. Великі каталоги організовані в деревоподібну структуру типу B-tree, що містить записи з вказівниками на зовнішні кластери з елементами каталогу, які не помістилися всередині запису MFT.

NTFS-розділ диска можна створити за допомогою програми *Disk Administrator*, яка знаходиться в підменю *Administrative Tools* меню *Programs* стартового меню.

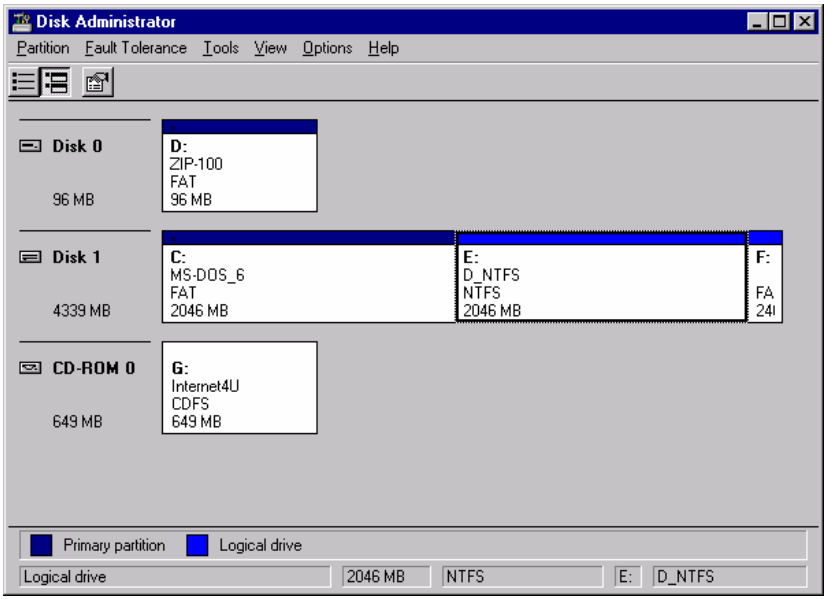


Рис. 6.3. Діалогове вікно програми *Disk Administrator*

Інший спосіб полягає у використанні команди *Format* з параметром */FS:NTFS*. Для перетворення існуючого FAT-розділу в формат NTFS слід користатися утилітою *Convert*. Перетворення файлової системи за допомогою *Convert* відбувається без втрат даних.

6.3. Доступ до файлів і каталогів. Поняття власника

Права на доступ до файлів і каталогів визначають, чи може користувач здійснити доступ до них, і якщо так – то яким чином. Володіння файлом чи каталогом дає змогу користувачеві змінювати права на доступ. Власником файла (каталогу) є користувач, який його створив. Адміністратор може заволодіти файлом (каталогом) без згоди власника, але не може повернути його назад попередньому власнику.

Надання прав на доступ до файлів (каталогів) є основою захисту інформації в Windows NT. Права на доступ до файлів (каталогів) визначаються в діалоговому вікні *File Permissions* (*Directory Permissions*). Для виклику цих діалогових вікон потрібно скористатись командою *Properties* відповідного контекстного меню потрібного файла (каталогу). У діалоговому вікні *File Properties* (*Directory Properties*) слід вибрати укладку *Security* і натиснути на кнопку *Permissions*. Розглянемо спочатку діалогове вікно File Permissions (див. рис.6.4). Воно складається з елементів *File*, *Owner*, *Name* і *Type of Access.*

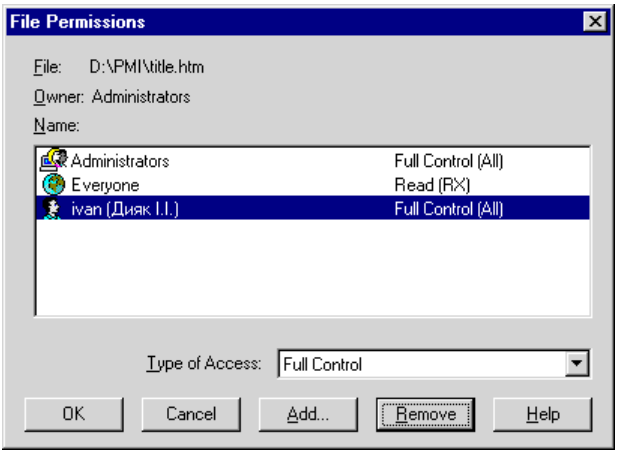


Рис. 6.4. Діалогове вікно *File Permissions*

У списку *Name* виводяться імена користувачів та груп, що мають право доступу до файла та тип доступу. Під час стоверення файла права доступу успадковуються від каталогу, в якому знаходиться файл. У списку *Type of Access* можна вибрати основні типи доступу до файла. Нижче в таблиці наведені типи доступу і пов'язані з ними дії над файлами.

Табл. 6.1. Типи доступу до файлів

	No Access	Read	Change	Full Control
Показувати дані файла		√	√	√
Показувати атрибути		√	√	√
Виконувати файл, якщо це програма		√	√	√
Показувати власника файла і типи доступу		√	√	√
Змінювати атрибути			√	√
Модифікувати файл			√	√
Знищувати файл			√	√
Змінювати власника файла і тип доступу				√

У списку *Type of Access* є елемент *Special Access*, за допомогою якого можна визначати спеціальні типи доступу. Нижче в таблиці наведені спеціальні типи доступу і пов'язані з ними дії.

Табл. 6.2. Спеціальні типи доступу до файлів

	Read	*Write*	*Execute*	*Delete*	*Change Permissions*	*Take Ownership*

Показувати власника файла і типи доступу	√	√	√			
Показувати дані файла	√					
Виконувати файл, якщо це програма			√			
Показувати атрибути	√		√			
Змінювати атрибути		√				
Модифікувати файл	√	√				
Знищувати файл				√		
Змінювати права доступу					√	
Володіти файлом						√

Надання прав доступу до каталогу здійснюється аналогічно до надання прав доступу до файлів. Діалогове вікно *Directory Permissions* (див. рис.6.5), окрім описаних вище елементів, містить додатково *Replace Permissions on Subdirectories* і *Replace Permissions on Existing Files*.

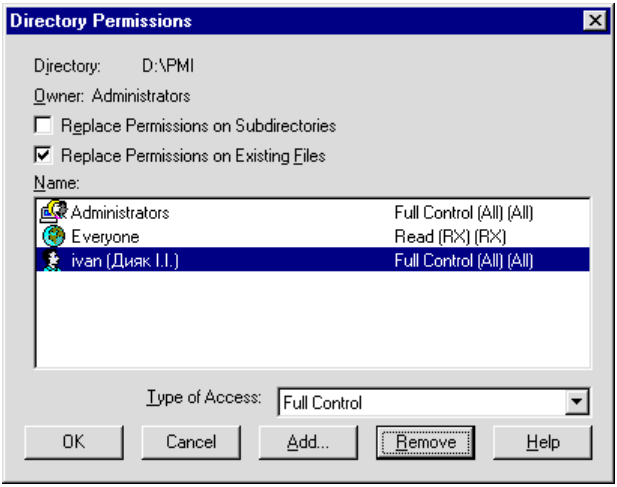


Рис. 6.5. Діалогове вікно *Directory Permissions*

Перший з них відмічається у випадку, коли потрібно перенести задані права доступу на всі вкладені каталоги (за замовчуванням не відмічений), а другий – на всі файли, що знаходяться в каталозі (відмічений за замовчуванням). У списку *Type of Access* можна вибрати один з нижченаведених видів доступу до каталогу.

Табл. 6.3. Права доступу до каталогу і дії, пов’язані з ними

	No Access	List	Read	Add	Add&Read	Change	Full Control
Показувати імена каталогів		√	√		√	√	√
Показувати атрибути каталогів, входити в підкаталоги		√	√	√	√	√	√
Змінювати атрибути, створювати підкаталоги				√	√	√	√
Показувати власника і права доступу		√	√	√	√	√	√
Знищувати каталог						√	√
Знищувати файл чи порожній підкаталог							√
Володіти, змінювати права доступу до каталогу							√
Показувати власника, права доступу та дані файла			√		√	√	√
Показувати та змінювати атрибути			√		√	√	√
Модифікувати, змінювати права доступу, знищувати, виконувати файл, якщо це програма						√	√

За замовчуванням користувач, який створив файл (каталог), є його власником. Файл (каталог) не можна передати комусь у власність, але власник може надати іншому користувачеві право стати власником цього ресурсу. Для того, щоб дізнатись хто є власником файла (каталогу) або стати власником (за наявності відповідних прав), слід у діалогову вікні *File Properties* перейти на укладку *Security* і натиснути кнопку *Ownership*.

6.4. Сумісне використання файлів та каталогів у мережі

Захист каталогів на NTFS-розділі, виділених для сумісного використання в мережі, складається з двох рівнів: мережного і локального. Віддалений користувач отримує права доступу, які є комбінацією прав доступу до спільних ресурсів і локальних обмежень NTFS. Це означає, що якщо користувач намагається модифікувати файл з мережі, то і локальні обмеження NTFS, і обмеження на сумісне використання повинні давати змогу це робити. Наприклад, якщо користувач *Ivan* має права доступу по мережі до каталогу типу Change, а локально для нього визначено права типу Read і Execute, то він може лише читати та виконувати файли, але не редагувати чи знищувати їх. Для каталогів на FAT-розділах захист можливий лише на мережному рівні.

Для виділення каталогу в сумісне використання, незалежно від того, на якому розділі (FAT чи NTFS) він знаходиться, треба, клацнувши його ім'я правою кнопкою миші, вибрати в контекстному меню команду Sharing. Після цього з'явиться діалогове вікно Directory Properties з активною укладкою Sharing (див. рис.6.6), в якому потрібно відзначити опцію Shared As і в полі Share Name вказати ім'я, під яким виділений ресурс буде доступним з мережі.

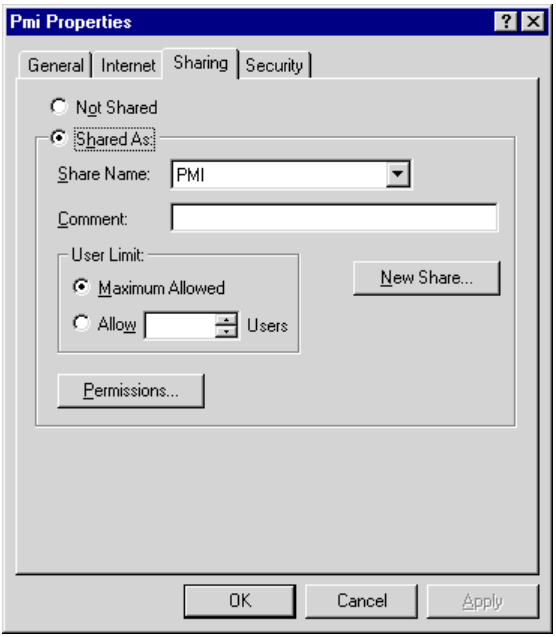


Рис. 6.6. Діалогове вікно *Directory Properties* з вкладкою *Sharing*

Параметр User Limit дає змогу вказати обмеження на максимальну кількість користувачів, що здійснюють одночасний доступ до ресурсу з мережі, а кнопка Permissions – вказати права доступу для окремих користувачів та груп за допомогою діалогового вікна Access Through Share Permissions. Це діалогове вікно за своєю структурою майже повністю ідентичне до діалогового вікна File Permissions. Права доступу зі списку Type of Access, і пов'язані з ними дії над файлами та каталогами, наведені в таблиці 6.4.

Табл. 6.4. Права доступу до каталогів з мережі

	No Access	Read	Change	Full Control

Показувати імена файлів та каталогів		√	√	√
Показувати дані у файлах та їх атрибути		√	√	√
Виконувати програми		√	√	√
Перехід у підкаталоги		√	√	√
Створювати підкаталоги і файли			√	√
Модифікувати файли			√	√
Змінювати атрибути файлів			√	√
Знищувати файли і підкаталоги			√	√
Змінювати права доступу				√
Ставати власником				√

Треба пам’ятати, що права доступу, визначені для каталогу сумісного використання, розповсюджуються на всі підкаталоги та файли в ньому. Крім того, Windows NT автоматично створює ресурс сумісного використовування *NETLOGON*, який вказує на каталог, де знаходяться файли сценаріїв реєстрації.

Один і той же каталог може бути виділений у сумісне використання декілька разів. При цьому кожного разу використовується нове ім’я ресурсу, а також є можливість вказати інші права доступу. Для повторного виділення каталогу в сумісне використання слід викликати описаним вище способом діалогове вікно *Directory Properties* з активною укладкою *Sharing* і натиснути на кнопку *New Share*.

Будь-який користувач груп *Administrators* та *Server Operators* може відмінити сумісне використання каталогу. Для цього слід у діалоговому вікні *Directory Properties* з активною укладкою *Sharing* відзначити опцію *Not Shared*.

Лекція 7. Використання командної стрічки та командних файлів в адміністративних цілях

7.1. Команди режиму командної стрічки

Хоча більшість адміністративних функцій виконуються за допомогою тієї чи іншої графічної програми (*User Manager*, *Server Manager* тощо), в Windows NT передбачений також і потужний набір функцій адміністрування, які працюють у режимі командної стрічки. Підтримуються майже всі можливості, що доступні в операційних системах DOS та OS/2 1.x. Увівши в командній стрічці команду *help*, можна одержати повний перелік внутрішніх команд програми ***cmd.exe***. Для одержання детальної інформації про конкретну команду слід ввести *help <ім'я команди>*. Windows NT підтримує командні файли з розширеннями ***.bat*** та ***.cmd***. Прикладом може бути імітація Unix-команди *cp*, реалізована у вигляді командного файла *cp.bat* з використанням команди *choice*:

```
if exist %2
goto ask_user
do_copy:
copy %1 %2
exit
ask_user:
choice /c:yn File exists, overwrite it
if ERRORLEVEL 1 goto do_copy
```

Введення користувачем команди *cp a b*, за умови, що файл "b" існує, викличе формування запиту: *File exists, overwrite it [Y, N] ?* Якщо користувач натисне клавішу Y, то файл буде записано по вже існуючому файлу "b". В іншому випадку робота програми буде перервана.

7.2. Адміністративні мережні команди

Для адміністрування мережі найбільш важливими є мережні команди групи *net* та планувальник команд *at*.

Можливості команди *net* дають змогу використовувати її в адміністративних цілях у командних файлах і сценаріях реєстрації. Для того, щоб отримати список мережних команд, треба в командній стрічці ввести *net*. Для отримання детальної інформації про конкретну команду наберіть *net help <ім'я команди>*.

Мережні команди можна умовно поділити на дві групи: команди для керування ресурсами, які знаходяться в сумісному використанні, і команди, призначені тільки для адміністративних цілей. Розглянемо спочатку команди першої групи.

7.3. Команди керування виділеними ресурсами

Синтаксис цих команд повністю збігається із синтаксисом одноіменних команд у мережах на базі систем LAN Manager, LAN Server, MS-Net, Windows 95, тому користувачі, які знайомі з цими системами можуть відразу користуватися командами *net* і в Windows NT. Для перегляду

списку ресурсів мережі використовується команда *net view*. Запуск цієї команди без аргументів призведе до виведення на екран списку усіх комп'ютерів мережі. Для того, щоб взнати які спільно використовувані ресурси є на конкретному комп'ютері, введіть команду *net view <ім'я комп'ютера>*. У мережах з декількома доменами чи робочими групами перелік доменів та робочих груп можна отримати ввівши команду *net view /domain*, а список комп'ютерів конкретного домену (робочої групи) – за допомогою команди *net view /domain:<ім'я домену>*.

Спільне використання каталогів ініціюється з командної стрічки командою *net share <ім'я каталогу в мережі>=<ім'я каталогу, який виділяється для спільного користування>*. Наприклад, команда *net share my_folder=d:\personal* забезпечує виділення для спільного використання в мережі папки personal під іменем my_folder. Для обмеження кількості користувачів, які можуть одночасно працювати з цим ресурсом, слід вказати параметр */users:<кількість користувачів>*. Команда *net share* без параметрів видає інформацію про виділені ресурси того комп'ютера, з якого вона введена. Слід зауважити, що за допомогою команди *net share* не можна виділити для спільного використання принтер.

Для встановлення зв'язку з виділеними для спільного користування ресурсами призначена команда *net use*. Введена без параметрів, ця команда видає список виділених ресурсів, з якими зв'язок вже встановлено. Синтаксис команди *net use* для встановлення зв'язку з ресурсом має такий вигляд: *net use <ім'я пристрою> <повне ім'я ресурсу в мережі>*. Наприклад, для того, щоб під'єднатися до каталогу Public на комп'ютері Pmiserver, слід ввести команду *net use Z: \\Pmiserver\Public*. Команда *net use* з параметром */delete* скасовує спільне використання ресурсу. Наприклад, команда *net use /delete Z:* відміняє спільне використання ресурсу *\\Pmiserver\Public* і звільняє ім'я пристрою Z. Якщо зв'язок необхідно встановлювати і для наступних сеансів роботи, команду *net use* слід використовувати з параметром */Persistent:Yes*, у протилежному випадку треба вказати */Persistent:No.* Якщо ресурс, з яким встановлюється зв'язок, захищений паролем, то після повного імені ресурсу в мережі слід записати пароль або символ *, який дає системі вказівку вимагати введення пароля користувачем. Задання параметра */user:<ім'я користувача>* в команді *net use* дає змогу встановити зв'язок з ресурсом, використовуючи ім'я, що відмінне від того, під яким користувач зареєстрований в системі.

7.4. Команди для адміністративних цілей

Використовуючи ці команди в командних файлах або сценаріях реєстрації, можна розв'язувати усі розглянуті у попередніх лекціях задачі адміністрування. Команди цієї групи характеризуються наявністю великої кількості параметрів, детальний опис яких можна знайти, наприклад у [2]. Тому опишемо коротко тут лише найчастіше вживані команди.

Під час виконання процедур розподіленого резервного копіювання та деяких інших важливих мережних операцій надзвичайно важливо, щоб усі системні годинники комп'ютерів мережі були синхронізовані. Для цього використовують команду *net time*. Без параметрів ця команда виводить системний час. Команда *net time \\ім'я_комп'ютера* виводить системний час комп'ютера з вказаним ім'ям. Команда *net time /domain* виводить системний час PDC домену. Використання ключового слова */set* дає змогу визначити час у відповідності з системним часом на комп'ютері, якому адресовано запит. Наприклад, команда *net time/domain/set* синхронізує робочу станцію (чи сервер) з показами системного годинника PDC.

У Windows NT є досить потужна система формування системних повідомлень, побудована на використанні команди *net send*. Команда *net send ivan Зателефонуй шефу!* пересилає мережею повідомлення *Зателефонуй шефу!* для користувача *ivan*. Якщо *ivan* - це ім'я комп'ютера, повідомлення отримає користувач цього комп'ютера. Команда *net send * <Текст>* викличе появу діалогового вікна *Message* з повідомленням *Текст* на всіх NT-комп'ютерах, що об'єднані в мережу. Використання параметра */domain* дає змогу передати повідомлення зареєстрованим користувачам цього домену. Параметр */ users* забезпечить отримання повідомлення всіма користувачами, що в цей час є під'єднаними до серверу.

Команди *net start, net stop*, *net pause, net continue* призначені для управління сервісами Windows NT. Команда *net start* без параметрів виводить перелік усіх сервісів, запущених в системі.

Команда *net session* дає змогу отримати перелік користувачів, які використовують ресурси серверу.

Команди *net accounts, net user*, *net group* та *net localgroup* використовуються для керування ОЗ користувачів та груп користувачів (найбільш характерна особливість адміністрування у Windows NT).

Команда *net accounts* без параметрів виводить інформацію щодо системної політики ведення облікових записів. Використана у формі *net accounts /domain*, ця команда виводить інформацію щодо облікової політики всього домену. Використовуючи параметри */force logoff: , /minpwlen: , /maxpwage: , / minpwage: , /uniquepw:* можна керувати всіма основними параметрами облікової політики окремого комп'ютера або всього домену.

Додати, знищити, змінити деякі параметри або переглянути ОЗ користувача можна за допомогою команди *net user*. Слід одразу зауважити, що ця команда не дає змоги керувати правами доступу, визначеними для ОЗ користувача. Це можна зробити лише в User Manager. Синтаксис цієї команди має вигляд:

*net user <ім'я користувача><пароль>(або *) один чи більше параметрів*

де *ім'я користувача* - це ім'я ОЗ користувача, з яким будуть проводитися певні операції, задані списком параметрів, *пароль* (якщо він вказаний) за-

дає пароль або змінює його, символ * формує запрошення для введення пароля (дуже корисний метод у тому випадку, коли потрібно створити командний файл для введення нових паролів і при цьому уникнути можливих порушень захисту, викликаних безпосередньою наявністю пароля у файлі).

Розглянемо коротко основні параметри команди *net user*. Параметр */domain* визначає виконання заданих операцій на PDC домену Windows NT. На робочій станції Windows NT або на NT-сервері, сконфігурованому не як контролер домену, дія команди *net user* без параметра */domain* розповсюджується лише на локальний комп'ютер. Параметр */add* додає ОЗ користувача в базу даних SAM, а параметр */delete* знищує ОЗ. Параметр */add* може доповнювати аргумент */active:*, який набуває значень *yes* або *no*. Цей аргумент відповідно активує або блокує ОЗ. Параметр */expires:*, після якого вказано дату або ключове слово *never*, визначає термін дії ОЗ. Наприклад:

*net user ivan * /add /expires:12/25/99*

створює новий ОЗ з іменем *ivan*, з паролем, введеним користувачем під час виконання цієї команди, термін дії якого завершується 25 грудня 1999 року.

Параметр */homedir:* задає місцезнаходження домашнього каталогу користувача, причому вказаний тут каталог повинен бути попередньо створений. Параметри */profilepath:* і */scriptpath:* задають шляхи до файлів профілю користувача та сценарію реєстрації, відповідно. Функціонально задання цих параметрів еквівалентне аналогічним параметрам в *User Manager*. За допомогою параметра */passwordchg:* з ключовим словом *yes(no)* можна надати право (заборонити) користувачеві змінювати свій пароль. Параметр */times:* з ключовим словом *all* або датою задає період часу, в межах якого користувач має змогу реєструватися в системі. Формат дати - *день-день, година-година*. Дні тижня можна задавати повністю або скорочено, а години - як у дванадцятигодинному, так і двадцятичотиригодинному форматах. Наприклад, команда

net user ivan /times:monday-friday, 9.00-15.00

дає змогу користувачеві з іменем *ivan* реєструватися в будь-який робочий день тижня з 9.00 до 15.00.

Керування групами користувачів здійснюється за допомогою команд *net group* та *net localgroup*. Дія команди *net localgroup* розповсюджується лише на локальний комп'ютер, (зокрема і NT Server) на якому вона виконується. Команда *net localgroup <ім'я групи> /add* створює в базі даних SAM ОЗ локальної групи, а команда *net localgroup <ім'я групи> /delete* знищує ОЗ групи. Параметр */domain* вказує на необхідність виконувати цю команду на PDC домену. Команда *net group* створює глобальні групи домену і може виконуватися лише на комп'ютері з Windows NT Server. Команда *net group <ім'я групи> /add* створює нову глобальну групу, а команда *net group <ім'я групи> /delete* - знищує глобальну групу.

Зауважимо, що параметр */domain* у команді *net localgroup* ігнорується, якщо вона виконується в Windows NT Server, оскільки NT-сервери виконують свої операції на головному контролері домену за замовчуванням.

Команди *net localgroup* та *net group* можна використовувати для додавання (вилучення) окремих користувачів у глобальні та локальні групи. Наприклад, команда

net group "Domain Admins" vit /add

додає ОЗ користувача *vit* в глобальну групу *Domain Admins*. Команда

net localgroup administrators alex /delete

з локальної групи *administrators* на локальному сервері Windows NT вилучає ОЗ користувача *alex*. Якщо ім'я користувача не вказано, то команди *net localgroup, net group* виводять список груп або членів заданої групи.

7.5. Планувальник команд

Команда *at* дає змогу планувати виконання команд та командних файлів на віддалених комп'ютерах. Для цього на відповідному комп'ютері має бути запущено планувальник, наприклад, за допомогою команди *net start scheduler*. Виконання команди *at* без параметрів виводить перелік усіх запланованих команд. Команда *at* має такий синтаксис:

at \\ім'я_комп'ютера час "командна стрічка"

де *\\ім'я_комп'ютера* визначає комп'ютер, на якому має бути виконана команда (якщо ім'я не вказано, команда буде виконана на локальному комп'ютері), а параметр *час* - час виконання команди. Для цього параметра можна використовувати різні варіанти: */every:* , за яким можуть бути подані день тижня (наприклад *monday* або *m*) або число місяця; */next:* , що забезпечуватиме виконання команди в найближчий вказаний день. Для кращого розуміння наведемо кілька прикладів використання цієї команди:

at \\Pmiserver 9:30 tomorrow "net send Pmiserver Доброго ранку"

at 24:00 /NEXT: friday BACKUP.BAT

at 9:00 /EVERY: m, tu,w, th, f "net time/domain/set"

Параметр */delete* дає змогу вилучити завдання з вказаним ідентифікатором ID (ID завдання відображається в переліку, який формує команда *at* без параметрів), а без ідентифікатора - вилучити всі завдання на вказаному комп'ютері.

Список літератури:

1. Зубанов Ф.В. Windows NT - "выбор профи". - М.:"Русская Редакция", 1996.- 392с.

2. Рули Дж., Мэсвин Д., Хендерсон Т., Хеллер М. Сети Windows NT 4.0. - Киев: BHV, 1997.- 800с.

3.Ресурсы Windows NT . СПб.:BHV – Санкт-Петербург, 1996. –720 с.

4.Томас С., Пламли С. Создание INTRANET-сети в Windows NT 4.0. - Киев: BHV, 1997.- 400с.

5.Windows NT. Учебный курс Microsoft. -М.: "Русская редакция"-1997.-400 с.
6.http:\\www.microsoft.com

Серія науково-методичних матеріалів
"Побудова та адміністрування Intranet-мереж"
складається з наступних частин:

1.Основи мережних технологій
2.Адміністрування мереж Windows NT

Видавничий центр
Львівського державного університету ім. Івана Франка.
290602 Львів, вул. Університетська, 1.
