С. М. Захарченко, О.І. Суприган

ОСНОВИ СИСТЕМНОГО АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ НА БАЗІ ОС WINDOWS

Міністерство освіти і науки України
Вінницький національний технічний університет

С. М. Захарченко, О.І. Суприган

ОСНОВИ СИСТЕМНОГО АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ НА БАЗІ ОС WINDOWS

Затверджено Вченою радою Вінницького національного технічного університету як навчальний посібник для студентів спеціальностей «Інтелектуальні системи прийняття рішень», «Комп'ютерні системи та мережі», «Захист інформації в комп'ютерних системах та мережах», «Адміністративний менеджмент у сфері захисту інформації з обмеженим доступом». Протокол № 11 від « 2 » липня 2007 року.

Вінниця ВНТУ 2008

УДК 681.3.004.7 (075)
З 38

Р е ц е н з е н т и :

Лужецький В. А., доктор технічних наук, професор
Петух А. М., доктор технічних наук, професор
Ревенок В. І., кандидат технічних наук, доцент

Рекомендовано до видання Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України

З 38 **Захарченко С. М., Суприган О. І.**
Основи системного адміністрування комп'ютерних мереж на базі ОС Windows. Навчальний посібник. – Вінниця: ВНТУ, 2008.– 100 с.

В даному навчальному посібнику розглядаються сучасні підходи до конфігурування локальних мереж із використанням операційної системи Windows. В посібнику подаються особливості налаштувань серверної та клієнтської частин ОС Windows, а також основні принципи керування операційною системою з точки зору безпеки, пояснюються особливості логічної організації ОС Windows та команд для конфігурування серверної частини, розглядаються загальні питання щодо діагностування комп'ютерних мереж.

Навчальний посібник призначений для студентів спеціальностей «Інтелектуальні системи прийняття рішень», «Комп'ютерні системи та мережі», «Захист інформації в комп'ютерних системах та мережах», «Адміністративний менеджмент у сфері захисту інформації з обмеженим доступом», курсів «Системне адміністрування», «Захист комп'ютерних мереж», «Корпоративні та загальнодоступні мережі», «Автоматизовані засоби безпеки» і може бути рекомендований для студентів денної та заочної форми навчання.

УДК 681.3.004.7 (075)

ЗМІСТ

ВСТУП 6
Розділ 1 Планування операційної системи 7
1.1 Розміщення системних файлів та файлів користувачів 7
1.1.1 Розміщення операційної системи на сервері 7
1.1.2 Розміщення додатків на сервері 8
1.1.3 Збереження робочих файлів 10
1.2 Служба каталогів Active Directory 11
1.2.1 Базові терміни і концепції 13
1.2.1.1 Сфера впливу 13
1.2.1.2 Простір імен 13
1.2.1.3 Об'єкт 13
1.2.1.4 Контейнер 14
1.2.1.5 Дерево 14
1.2.1.6 Ім'я 14
1.2.1.7 Контексти імен і розділи 15
1.2.1.8 Домени 15
1.2.1.9 Дерево доменів 15
1.2.1.10 Ліс 16
1.2.1.11 Вузли 17
1.2.1.12 Схема 17
1.2.1.13 Модель даних 17
1.2.1.14 Глобальний каталог 17
1.2.2 Архітектура Active Directory 18
Контрольні питання до розділу 1 19
Розділ 2 Керування операційною системою 20
2.1 Система безпеки Windows 2003 20
2.1.1 Базові відомості про шифрування 21
2.1.1.1 Симетричне шифрування 21
2.1.1.2 Асиметричне шифрування 21
2.1.1.3 Цифрові підписи 21
2.1.1.4 Сертифікати 21
2.1.2 Протокол аутентифікації Kerberos 22
2.1.2.1 Основи Kerberos 22
2.1.3 Безпека і Active Directory 23
2.1.4 Довірчі відносини між доменами 24
2.1.5 Елементи безпеки системи 24
2.1.5.1 Облікові записи користувачів і груп 24
2.1.5.2 Локальна політика безпеки 27
2.1.5.3 Доменна політика 29
2.1.5.4 Редактор конфігурацій безпеки 30
2.1.5.5 Функції редактора конфігурацій безпеки 31

2.2 Контроль реєстру робочої станції 31
2.2.1 Використання системних політик 32
2.2.2 Шаблони системної політики 32
2.2.3 Файли системної політики 33
2.2.3.1 Створення файлів політики 34
2.2.3.2 Пріоритети політики 34
2.2.4 Визначення правил політики 35
2.2.5 Обмеження діяльності робочої станції за допомогою системної політики 36
2.2.5.1 Обмеження додатків 36
2.2.5.2 Блокування інтерфейсу 37
2.2.5.3 Захист файлової системи 40
2.2.6 Застосування системної політики 41
2.2.6.1 Віддалене редагування реєстру 41
2.2.6.2 Групові політики Windows 41
2.3 Керування робочим середовищем користувачів 42
2.3.1 Відображення дисків 42
2.3.2 Профілі користувачів 43
2.3.3 Створення переміщуваних профілів 45
2.3.4 Створення обов’язкових профілів 47
2.3.5 Реплікація профілів 48
2.3.6 Створення мережевого профілю користувача за замовчуванням 48
2.3.7 Ініціатива нульового адміністрування Microsoft для Windows 48
2.3.8 Компоненти ZAK 49
2.3.9 IntelliMirror 50
Контрольні питання до розділу 2 51
Розділ 3 Файлові системи Windows NT 52
3.1 Файлова система FAT 52
3.1.1 Дисковий розділ FAT 52
3.1.2 Файлова система FAT32 54
3.2 Файлова система NTFS 54
3.2.1 Головна файлова таблиця 55
3.2.2 Цілісність даних і відновлення в NTFS 55
3.2.3 Довгі і короткі імена файлів 56
3.2.4 Компресія файлів і каталогів 56
3.2.5 Створення і модифікація розділів диска 57
3.2.6 Перетворення існуючого розділу у формат NTFS 58
3.3 Розподілена файлова система 58
3.3.1 Переваги DFS 58
3.3.2 Технічний огляд розподіленої файлової системи 59
3.3.3 Робота з DFS 61
3.4 Файлова система із шифруванням 62
3.4.1 Архітектура EFS 62

3.4.2 Робота з EFS 63
3.5 Квотування дискового простору 65
3.5.1 Права на доступ до файлів і каталогів. Поняття власника 66
3.5.2 Надання і заборона доступу до файлів 66
3.5.3 Надання прав на доступ до каталогів 67
3.5.4 Володіння каталогами і файлами 69
Контрольні питання до розділу 3 69
Розділ 4 Програмні засоби діагностування комп'ютерної мережі 70
4.1 Утиліти операційної системи Windows 70
4.1.1 NET 70
4.1.2 NET CONFIG 70
4.1.3 NET DIAG 72
4.1.4 NET START і NET STOP 72
4.1.5 Інспектор мережі 75
4.1.5.1 З'єднання з віддаленою системою 75
4.1.5.2 Використання вікна підключень 76
4.1.5.3 Використання вікна загальних папок 76
4.1.5.4 Використання вікна відкритих файлів 77
4.1.5.5 Спостереження за мережевою активністю в Windows NT/2000/ XP/2003/Vista 77
4.1.5.6 Утиліти Server Manager для Windows NT 77
4.1.6 Web Administrator 77
4.1.7 NetMeeting 78
4.2 Утиліти TCP/IP 79
4.2.1 PING 79
4.2.2 Traceroute 82
4.2.3 Route 84
4.2.4 Netstat 84
4.2.5 Nslookup 86
4.2.6 Ipconfig 87
4.3 Аналізатори мережі 88
4.3.1 Фільтрація даних 89
4.3.2 Агенти 90
4.3.3 Аналіз трафіка 91
4.3.4 Аналіз протоколів 91
4.3.5 Тестери кабелю 92
Контрольні питання до розділу 4 93
Завдання для студентів заочної форми навчання 94
Завдання для лабораторних робіт 95
Література 99

ВСТУП

Незважаючи на те, що корпоративні мережі зазвичай використовують безліч операційних систем, особливо на серверах, на більшості робочих станцій, призначених для користувача, зазвичай установлена одна із версій Windows. Інтерфейс Windows є інтуїтивним і дружнім, немає жодних сумнівів у тому, що адміністрування серверів та сотень тисяч робочих станцій Windows являє собою вкрай масштабну задачу. Операційні системи Windows 95, 98, ME, Windows NT Workstation, Windows 2000/XP Professional, Windows Server 2003 та Windows Vista містять різні інструменти, які адміністратори мереж можуть застосовувати для полегшення процесів установлення, керування й обслуговування операційних систем великої кількості серверів і робочих станцій.

В даному навчальному посібнику розглядаються базові принципи адміністрування мережевої операційної системи Microsoft Windows. Хоча на сьогоднішній день використовуються різноманітні версії цієї системи починаючи з Windows 95 і закінчуючи Windows Vista, найпоширенішими версіями для робочих станцій є Windows 2000 Professional та Windows XP. Щодо серверного програмного забезпечення – це Windows 2000 Server та Windows 2003 Server. Саме тому в посібнику робиться наголос на ці версії Windows.

Перший розділ присвячено загальним принципам планування операційної системи, зокрема розглядаються питання розташування файлів користувачів та операційної систем на диску. В цьому розділі також розглянуто базові концепції Active Directory – бази даних мережевих ресурсів, яку використовує Microsoft.

В другому розділі розглядаються питання керування операційною системою, а саме створення і керування обліковими записами користувачів, використання профілів та системних політик для керування середовищем та можливостями користувачів на робочих станціях. А також описано базові принципи безпеки операційної системи.

В третьому розділі розглянуто файлові системи, які підтримують сучасні версії Windows. Більш детально розглянуто файлові системи, які розроблено безпосередньо Microsoft і використання яких дозволяє отримати найкращий результат з точки зору захищеності, продуктивності та функціональності системи. Крім NTFS розглянуто також розподілену файлову систему DFS та шифровану файлову систему EFS.

Останній розділ посібника містить інформацію про засоби діагностування комп'ютерних мереж, розглядаються найпоширеніші команди контролю доступності окремих вузлів, перевірки конфігурації протокольного стека, а також загальні принципи моніторингу трафіка.

Розділ 1
Планування операційної системи

1.1 Розміщення системних файлів та файлів користувачів

Однією з головних задач будь-якого адміністратора мережі є ухвалення рішення про те, де у мережі будуть зберігатися дані. Робочим станціям мережі потрібен доступ до файлів операційної системи, додатків і робочих файлів, тому визначення місць розташування цих елементів є найважливішою частиною процесу створення стабільної і безпечної мережі. Деякі адміністратори взагалі не контролюють, де користувачі зберігають свої робочі файли. На щастя, більшість додатків, що працюють у середовищі Windows, установлюються за замовчуванням у каталог C:\Program Files локального диску, і це вже забезпечує деяку міру послідовності. Деякі додатки навіть створюють робочі каталоги за замовчуванням на локальному диску, однак залишати користувачів наодинці з їх власними пристроями, коли мова йде про збереження файлів даних, зазвичай є вкрай небезпечною практикою. Багато користувачів не мають узагалі жодних чи мають дуже мало знань про структуру каталогів своїх комп'ютерів, а також не мають досвіду керування файлами. Це може призвести до того, що файли для різних додатків виявляться безладно «звалені» в один загальний каталог і залишені без будь-якого захисту від випадкового видалення або пошкодьження.

1.1.1 Розміщення операційної системи на сервері

В перших версіях Windows запуск операційної системи з диска сервера був практичною альтернативою установлення ОС на кожну робочу станцію. Збереження файлів операційної системи на сервері дозволяло адміністратору не тільки запобігти їхньому ушкодженню чи випадковому видаленню, але й оновлювати версію ОС для всіх робочих станцій одночасно. Подібне рішення також допомагає заощаджувати дисковий простір робочих станцій.

В даний час просте установлення стандартної операційної системи на диск сервера не вважається практичним. Робоча станція, що використовує операційну систему Windows, повинна завантажити багато мегабайтів інформації тільки для запуску системи. Якщо помножити цю цифру на загальну кількість робочих станцій мережі, що обчислюється сотнями, можна легко уявити, що загальний обсяг мережевого трафіка, який генерується при цьому, ляже тяжким тягарем навіть на найшвидшу мережу. Крім того, наявність дискового простору не є проблемою, коли найзвичайніші робочі станції оснащуються жорсткими дисками ємністю від 40 до 500 Гбайт інформації. Установлення операційної системи на локальний диск в більшості випадків є більш оптимальним рішенням.

З іншого боку, у даний час з'явився цілий ряд нових технологій, які підвищують практичність завантаження і виконання операційної системи Windows із сервера. Проте у нинішньому варіанті робочі станції не завантажують операційну систему тільки з диска сервера. Замість цього робочі станції функціонують як клієнти-термінали, які з'єднуються із сервером терміналів. Операційна система і додатки робочої станції фактично виконуються сервером, у той час як функції термінала вичерпуються винятково введенням/виведенням. У результаті, робочі станції вимагають мінімальної кількості ресурсів, тому що сервер бере на себе основну частину обчислювального навантаження.

При використанні подібної схеми термінали можуть бути відносно слабкими комп'ютерами, наприклад, машинами з процесором Celeron D310, набором системної логіки Intel 865, ОЗУ 512 Мбайтів, відеоадаптером ATI 9600, що виконують програму емуляції терміналу, або ж спеціалізованими терміналами Windows, розробленими для запуску винятково клієнтського програмного забезпечення. У будь-якому випадку вартість подібної робочої станції навіть близько не можна порівнювати з ціною нового персонального комп'ютера, апаратне забезпечення якого достатнє для виконання індивідуальної копії Windows.

Експлуатація мережі Windows, заснованої на терміналах, докорінно відрізняється від обслуговування стандартної ЛОМ, і даний варіант не можна назвати альтернативою для тих мереж, що уже використовують повні версії операційних систем Windows на своїх робочих станціях. Однак, якщо формується нова мережа чи проводиться масштабне розширення, використання терміналів Windows може стати одним з тих варіантів рішення, які варто розглянути.

1.1.2 Розміщення додатків на сервері

Запуск додатків з диска сервера замість диска робочої станції є ще одним способом забезпечення стабільної робочої конфігурації для користувачів і зведення до мінімуму навантаження із адміністрування мережі. У найпростішій формі процес зводиться до установлення додатка звичайним чином із вказанням каталогу мережевого диска замість локального каталогу як місця розташування файлів програми. Однак додатки Windows ніколи не відрізнялися простотою, тому у дійсності цей процес виглядає набагато складніше.

Запуск додатків з диска сервера має як переваги, так і недоліки. Позитивним фактором у випадку з розміщенням на сервері операційної системи можна назвати економію простору локальних дисків, захист файлів додатків від ушкодження та видалення, а також можливість поліпшення й обслуговування єдиної копії додатка, а не індивідуальних копій на кожній робочій станції. Серед недоліків на перший план виступає той факт, що додатки, розміщені на сервері, зазвичай працюють порівняно повільніше, ніж

їхні локальні аналоги, а також генерують істотний обсяг мережевого трафіка і не можуть функціонувати, якщо сервер несправний чи недоступний з інших причин.

В часи використання ОС MS DOS додатки були самодостатніми і зазвичай складалися не більш ніж з одного програмного каталогу, що містив усі файли даного додатка. Тоді можна було установити додаток на сервер і дозволити іншим системам використовувати його, просто запускаючи файл, що виконується. Сьогоднішні додатки Windows набагато складніші, і програма їхньої інсталяції не вичерпується простим копіюванням файлів. Крім програмних файлів Windows включає певні установлення системного реєстру, наявність деяких DLL-файлів Windows, що повинні бути наявними на локальному диску, а також процедуру створення рядків у меню кнопки Start (Пуск) або піктограм, необхідних для запуску додатка.

Якщо є бажання спільно використовувати декількома робочими станціями додаток, розміщений на сервері, то необхідно провести його повне установлення на кожній робочій станції. Це робиться для того, щоб бути упевненим, що кожна робоча станція має відповідні файли Windows, установлення реєстру і піктограми, необхідні для роботи додатка. Один із способів практичної реалізації додатка, розміщеного на сервері, полягає в проведенні повної інсталяції програми на кожну робочу станцію із вказанням імені того самого каталогу сервера як місця розташування файлів програми в кожному окремому випадку. Таким чином, кожна робоча станція одержить усі необхідні файли і модифікації, а на сервері залишиться лише одна копія файлів додатка.

Іншою важливою проблемою є здатність підтримувати індивідуальні параметри конфігурації для кожної робочої станції, що одержує доступ до додатка. Наприклад, якщо один з користувачів модифікує інтерфейс спільно використовуваного додатка, дуже небажано, щоб ці зміни відбивалися на інших користувачах. У результаті кожний з користувачів додатка повинен підтримувати власну копію параметрів конфігурації даного додатка. Це залежить від того, де саме даний додаток зберігає свої конфігураційні установлення. Якщо, наприклад, установлення зберігаються в системному реєстрі або у ini-файлі Windows, у процесі інсталяції буде створена окрема конфігурація для кожної робочої станції. Однак, якщо за замовчуванням установлення конфігурації додатка розміщуються разом з файлами програми на сервері, то варто зробити ряд кроків, спрямованих на те, щоб не допустити ситуації, коли зміни, внесені одним користувачем, анулюють зміни інших користувачів.

У деяких випадках існує можливість конфігурування додатка для збереження установлень конфігурації в альтернативному місці, що дозволяє перемістити їх на локальний диск кожної з робочих станцій або в індивідуальний каталог кожного користувача на сервері. Якщо такої можливості

немає, то додаток не можна вважати придатним для спільного вико ристання в мережі.

У багатьох випадках найпрактичнішим способом виконання додатків, розміщених на сервері, є застосування додатка, що має свої власні мережеві можливості. Наприклад, Microsoft Office дозволяє створювати на сервері точку керованої інсталяції (administrative installation point), яку можна потім використовувати для установлення додатка на робочі станції. Проводячи кожну інсталяцію, можна вибирати, чи будуть файли додатка копіюватися на локальний диск, запускатися з диска сервера або розподілятися між сервером і робочою станцією.

1.1.3 Збереження робочих файлів

У більшості сучасних мереж з операційною системою Windows як файли операційної системи, так і додатки установлюються на локальних комп'ютерах. Однак, тільки від адміністратора мережі залежить ухвалення рішення про те, де саме будуть зберігатися файли даних, які створюються користувачами. При рішенні даного питання варто звертати особливу увагу на деякі принципові моменти, а саме: доступність цих файлів для користувачів і їхня безпека. Природно, що користувачі повинні одержувати доступ до своїх файлів даних, але існують також файли, які повинні спільно використовуватися багатьма користувачами. Важливі файли даних також повинні бути захищені від модифікації і видалення неавторизованими користувачами і до того ж дублюватися на альтернативному носії з метою страхування від непередбачуваних обставин, наприклад, виходу диска з ладу.

Робочі файли можуть мати різний формат, що не може не впливати на те, яким способом їх слід зберігати. Наприклад, документи індивідуальних користувачів, створені за допомогою текстових редакторів чи електронних таблиць, призначені для використання тільки однією людиною в певний момент часу, у той час як бази даних підтримують одночасний доступ декількох користувачів. У більшості випадків файли баз даних зберігаються на комп'ютерах, які виконують функції серверів баз даних, тому адміністратори можуть регулювати доступ до них за допомогою засобів файлової системи та регулярним резервним копіюванням. Інші типи файлів можуть вимагати додаткового планування політики доступу до них.

Операційні системи Windows дозволяють користувачам зберігати свої документи як на локальних дисках, так і на дисках сервера, і мати можливість спільного використання документів з іншими користувачами мережі. Однак є досить вагомі причини, відповідно до яких більш правильним рішенням є збереження всіх робочих файлів на дисках сервера. Перша і найважливіша з цих причин полягає в тому, що так набагато простіше захищати файли від втрати через збій диска робочої станції. Сервери зазвичай оснащені захисними механізмами, такими як RAID-масиви чи дзеркальні томи. Крім того, сервери адаптовано для виконання резервного копіюван-

ня. Зрештою, сервери дозволяють зробити дані доступними в будь-який час, тоді як робоча станція може бути вимкнена при відсутності користувача.

Друга причина відноситься до керування доступом. Незважаючи на те, що і сервери, і робочі станції Windows мають подібні можливості надання прав конкретним користувачам, самі користувачі вкрай рідко мають достатній рівень навичок чи бажання ефективно захистити свої власні файли. Тому адміністраторам мережі набагато простіше керувати правами на одному сервері ніж на декількох робочих станціях. Ще одна вагома причина полягає в тому, що присутність дисків спільного використання у кожної робочої станції робить украй важким виявлення конкретної інформації в мережі. Якщо розглянути домен Windows і виявити там десятки або сотні комп'ютерів, кожний з яких має власні ресурси спільного використання, то можливо легко зрозуміти, наскільки складною буде задача визначення місця розташування конкретного файлу. Обмеження ресурсів спільного використання рамками невеликого числа серверів спрощує подібний процес.

У результаті найкращою стратегією для більшості мереж Windows є установлення операційної системи і всіх додатків на локальні диски робочих станцій зі збереженням усіх робочих файлів на серверах мережі. Найрозповсюдженіша практика полягає в створенні на сервері індивідуального каталогу для кожного користувача, причому користувачу надається повний контроль над власним каталогом. Потім необхідно сконфігурувати усі додатки для збереження робочих файлів у цьому каталозі за замовчуванням, щоб уся цінна інформація не зберігалась на локальному диску. Залежно від бажання користувачів мережі можна зробити домашні каталоги приватними (private), щоб тільки даний користувач мав доступ до свого каталогу, чи ж дозволити усім користувачам доступ типу «тільки читання» до індивідуальних каталогів інших користувачів. Це дозволить кожному користувачу спільно з іншими користувачами використовувати будь-який робочий файл, просто повідомивши йому ім'я і місце розташування цього файлу.

При створенні облікового запису користувача в домені Windows чи об'єкта користувача в Active Directory операційної системи Windows існує можливість одночасного створення індивідуального каталогу для даного користувача за допомогою діалогового вікна. За замовчуванням користувачам надається повний контроль над їх домашніми каталогами, а всім іншим доступ повністю заборонений.

При бажанні можна змінити ці права, щоб надати доступ до каталогу іншим користувачам мережі та адміністраторам.

1.2 Служба каталогів Active Directory

Згідно зі словником, каталог – це складений в певному порядку перелік однорідних предметів (книг, експонатів, товарів). Точно так, як і каталог виставки містить інформацію про експонати, каталог файлової системи

надає інформацію про файли. Відмінна особливість такого каталогу – можливість систематизації інформації, що зберігається, швидкого пошуку даних, а також додавання і розширення самого каталогу. Служба каталогів операційної системи зберігає інформацію про об'єкти системи і дозволяє маніпулювати ними.

Служба каталогів Active Directory (AD) – сервіс, інтегрований у Windows NT Server, починаючи з версії Windows 2000. Вона забезпечує ієрархічний вигляд мережі, нарощуваність і розширюваність, а також функції розподіленої безпеки. Ця служба легко інтегрується із Інтернетом, дозволяє використовувати прості і інтуїтивно зрозумілі імена об'єктів, придатна для використання в організаціях будь-якого розміру і легко масштабується. Доступ до неї можливий за допомогою таких інструментів як програма переглядання ресурсів Інтернету.

AD не тільки дозволяє виконувати різні адміністративні завдання, але і є постачальником різних послуг в системі. На наведеному нижче рисунку зображено основні функції служби каталогів.

В Active Directory концепція простору імен Інтернету об'єднана з системними службами каталогів, що дає можливість єдиним чином управляти різними просторами імен в гетерогенних середовищах корпоративних мереж. Основною AD є легкий протокол доступу до каталогу LDAP (lightweight directory access protocol), що дозволяє діяти за рамками операційної системи, об'єднуючи різні простори імен. Active Directory може включати каталоги інших застосувань або мережевих операційних систем, а також керувати ними, що значно знижує навантаження на адміністраторрів і накладні витрати.

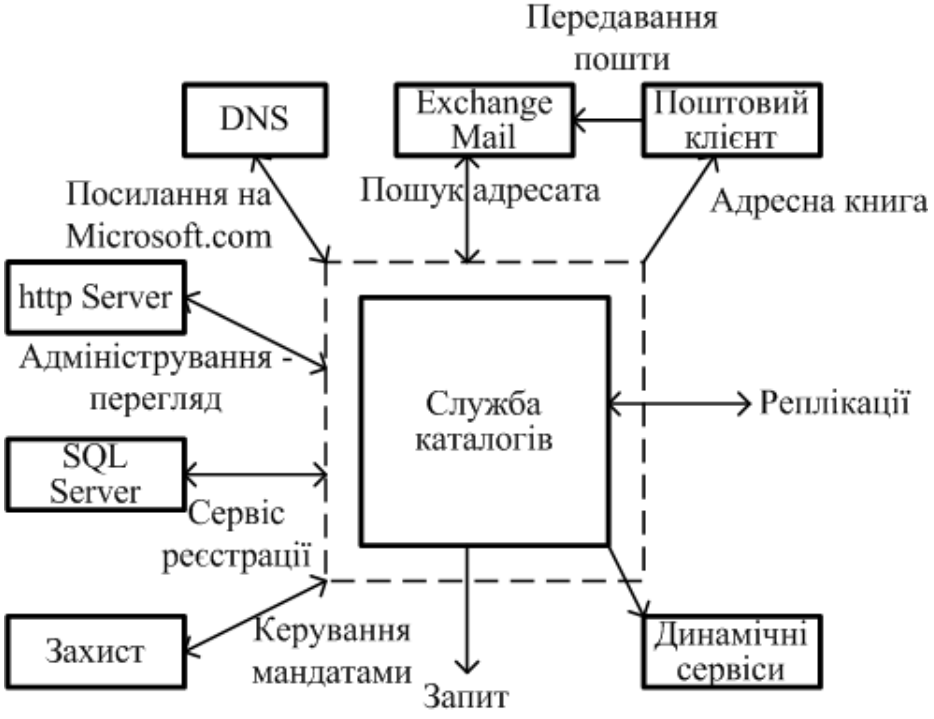

Рисунок 1.1 – Каталог – постачальник послуг в системі

LDAP – стандартний протокол доступу до каталогів (RFC1777) – був розроблений як альтернатива протоколу доступу X.500. В Active Directory підтримуються як LDAP v2, так і LDAP v3.

HTTP – стандартний протокол для відображення Web-сторінок. Active Directory дає можливість проглянути будь-який об'єкт у вигляді Web-сторінки. Розширення Internet Information Server, що постачаються разом із службою каталогу, перетворять запити до об'єктів каталогу в HTML-сторінки.

Active Directory дозволяє централізовано адмініструвати усі ресурси, будь-які довільні об'єкти і сервіси: файли, периферійні пристрої, бази даних, підключення до Web, облікові записи та ін. Як пошуковий сервіс використовується DNS. Всі об'єкти усередині домену об'єднуються в організаційні одиниці (OU), які становлять ієрархічні структури. У свою чергу, домени можуть об'єднуватися у дерева.

Ще одна особливість Active Directory – підтримка декількох сховищ, в кожному з яких може знаходитися до 10 мільйонів об'єктів. Зрозуміло, що при такій нагоді ця служба каталогів чудово проявляє себе як у малих мережах, так і у великих системах.

1.2.1 Базові терміни і концепції

1.2.1.1 Сфера впливу

Сфера впливу служби каталогів велика: будь-які об'єкти (користувачі, файли, принтери і ін.), сервери в мережі, домени і навіть глобальні мережі. Таким чином, можливості такої служби каталогів як AD практично безмежні, що робить її корисною на окремому комп'ютері, у великій мережі і в декількох мережах.

1.2.1.2 Простір імен

Як і будь-який каталог, Active Directory підтримує певний простір імен, тобто певну область, в якій дане ім'я може бути дозволено. Під дозволом імен розуміється процес, що дозволяє співставити ім'я із об'єктом, який йому відповідає, або з інформацією про даний об'єкт. Наприклад, у файловій системі ім'я файлу співставляється з розташування файлу на диску.

1.2.1.3 Об'єкт

Під об'єктом мається на увазі окремий набір атрибутів, відповідних чому-небудь конкретному: наприклад, користувачу, комп'ютеру або додатку. У атрибутах містяться дані про суб'єкт, що представлений даним об'єктом. Наприклад, атрибути користувача можуть включати його ім'я, прізвище, адреси домашньої та електронної пошти, сімейний стан, заробітну платню і т.д.

1.2.1.4 Контейнер

Контейнер – це об’єкт каталогу, який може містити в собі інші об’єкти (як, наприклад, тека – це контейнер для документів, а шафа – контейнер для тек). Контейнер каталогу є контейнером об’єктів каталогу.

1.2.1.5 Дерево

Деревом називається ієрархічна структура з об’єктів. Об’єкти, які розташовані на гілках цього дерева, називаються листям. У листях не міститься інших об'єктів, тобто листя не може бути контейнерами. Контейнерами є вузлові точки дерева (місця, з яких виходять гілки). Нерозривна частина дерева, яка включає всіх членів контейнера, називається суміжним піддеревом.

На рисунку 1.2 зовнішній вигляд дерева показує взаємозв’язки між об’єктами.

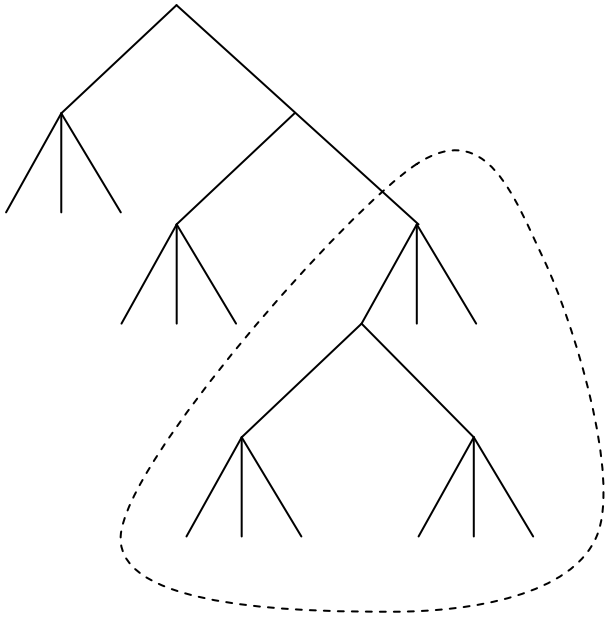

Рисунок 1.2 – Дерево та суміжне піддерево

1.2.1.6 Ім’я

Імена використовуються для ідентифікації об’єктів в Active Directory. Існує два види імен: унікальне ім’я DN (distinguished name) і відносно унікальне ім’я RDN (relatively distinguished name).

Унікальне ім’я об’єкта містить ім’я домену, у якому знаходиться об’єкт, а також повний шлях до цього об’єкта у ієрархії контейнера. Наприклад, унікальне ім’я для ідентифікації користувача Sergey Zakharchenko у домені VSTU.VINNICA.UA виглядатиме так:

/0=Internet/DC=UA/DC=VINNICA/DC=VSTU/CN=Users/CN=Sergey Zakharchenko

Відносне унікальне ім’я об’єкта – частина унікального імені, що є атрибутом об’єкта. У наведеному прикладі таким для об’єкту користувача Sergey Zakharchenko є

CN=Sergey Zakharchenko, а RDN його батьківського об’єкта – CN=Users.

1.2.1.7 Контексти імен і розділи

Active Directory складається з одного або декількох контекстів імен або розділів. Контекст імені – це будь-яке суміжне піддерево каталогу. Контексти імен є одиницями тиражування. Для будь-якого окремого сервера завжди є три контексти імен:

– схема;

– конфігурація (топологія тиражування і метадані, які відносяться до нього);

– один або декілька контекстів імен користувачів (піддерева, що містять дійсні об’єкти каталогу).

1.2.1.8 Домени

Домени є організаційними одиницями безпеки в мережі. Active Directory складається з одного або декількох доменів. Домен може охоплювати декілька фізичних точок. У кожному домені – своя політика безпеки; відносини домену з іншими також індивідуальні. Домени, об’єднані загальною схемою, конфігурацією і глобальним каталогом, утворюють дерево доменів. Декілька доменних дерев можуть бути об’єднані в ліс.

1.2.1.9 Дерево доменів

Дерево доменів складається з декількох доменів, що використовують одну і ту ж схему та конфігурацію, які створюють єдиний простір імен. Домени в дереві пов’язані між собою довірчими відносинами. Служба каталогів Active Directory складається з одного або декількох доменних дерев.

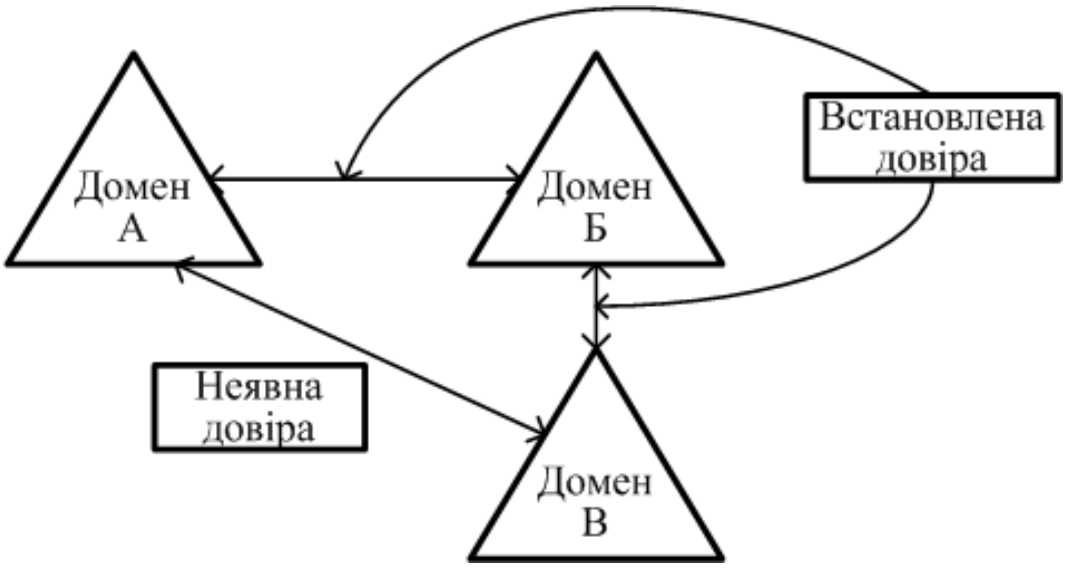

Рисунок 1.3 – Довірчі відносини Kerberos

Дерева можна розглядати як із погляду довірчих відносин, так із погляду простору імен.

У Windows 2003 довірчі відносини між доменами ґрунтуються на протоколі захисту Kerberos. Ці відносини транзитивні, тобто якщо домен А довіряє домену Б, а домен Б довіряє домену В, то домен А також довіряє домену В. На рисунку зображені домени з погляду довіри.

З іншого боку, домени можна розглядати з погляду унікальних імен. При цьому чітко простежується ієрархічна структура доменів і стає простішим пошук по усьому дереву.

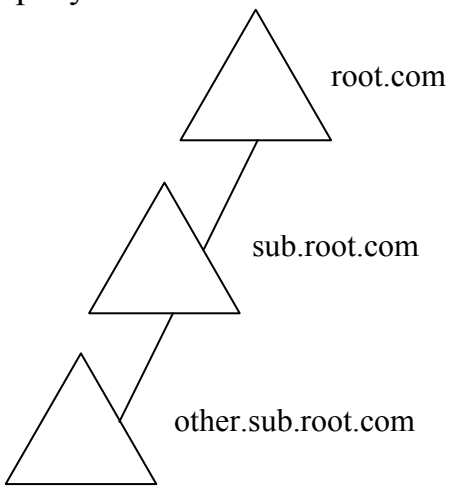

Рисунок 1.4 – Погляд на домени з точки зору простору імен

1.2.1.10 Ліс

Ліс – це набір несуміжних дерев, які не створюють єдиний простір імен. У той самий час всі дерева в лісі використовують одну і ту ж схему, конфігурацію і глобальний каталог і пов’язані між собою Kerberos – відносинами довіри. На відміну від дерев, у лісу немає певного імені. Він існує у вигляді поперечних посилань та ієрархічних довірчих відносин, відомих деревам, які його створюють. Для звернення до лісу використовується ім’я дерева в корені дерева, яке довіряє.

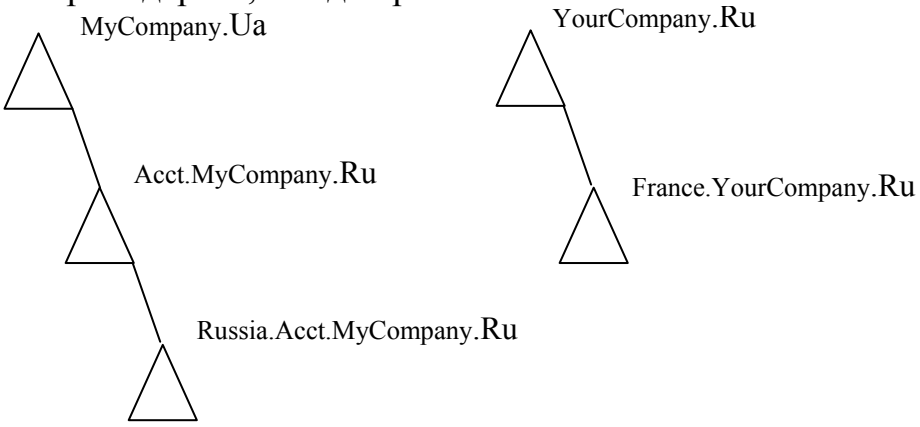

Рисунок 1.5 – Декілька дерев в лісі

1.2.1.11 Вузли

Вузол – це місце розташування в мережі серверів з Active Directory. Як вузли можуть виступати одна або декілька підмереж TCP/IP, що дозволяє конфігурувати доступ до каталогу і тиражування з урахуванням фізичної мережі. Коли користувач входить в мережу, сервер з Active Directory не треба довго шукати – адже він знаходиться в тому ж самому вузлі і робочій станції «відомо» як дістатися до нього за TCP/IP.

1.2.1.12 Схема

Схема Active Directory є набором екземплярів класів об'єктів, що зберігаються у каталозі. Це відрізняє її від схем інших каталогів, які, як правило, зберігаються в текстових файлах і прочитуються при завантаженні. Зберігання схеми в каталозі має ряд переваг. Наприклад, додатки можуть звертатися до каталогу і читати списки доступних об'єктів, а також динамічно змінювати схему, додаючи в неї нові атрибути і класи. Модифікація схеми супроводжується створенням або модифікацією об'єктів, що зберігаються у каталозі. Всі внесені зміни негайно стають доступні для інших додатків. Будь-які об'єкти схеми (втім, як і будь-які об'єкти Active Directory) захищені списками контролю доступу, що гарантує їх від змін особами, які не мають на це прав.

1.2.1.13 Модель даних

У основу моделі даних служби каталогів Active Directory покладена модель даних X.500. В каталозі зберігаються різні об'єкти, описані атрибутами. Класи об'єктів, які допустимо зберігати в каталозі, задаються схемою. Для кожного класу об'єктів в схемі визначені обов'язкові і можливі додаткові атрибути екземплярів класу, а також те, клас якого об'єкта може бути батьківським відносно того, що розглядається.

1.2.1.14 Глобальний каталог

Active Directory може складатися з декількох розділів або контекстів імен. В унікальному імені об'єкта міститься інформація, достатня для успішного пошуку копії розділу, що містить об'єкт. Проте часто користувачу або додатку невідомо ні унікальне ім'я об'єкта, ні розділ, де він може знаходитися. Глобальний каталог дозволяє користувачам і додаткам визначати положення об'єктів у дереві доменів Active Directory за одним або декількома атрибутами.

У глобальному каталозі міститься часткова копія кожного з контекстів імен користувачів, а також схема і конфігураційні контексти імен. Це означає, що в глобальному каталозі зберігаються копії всіх об'єктів Active Directory, але із скороченим набором атрибутів. До тих, що зберігаються, відносяться атрибути найчастіше використовувані при пошуку (наприклад, ім'я користувача, ім'я входу у систему і т. д.) і достатні для виявлення пов-

ної репліки об’єкта. Глобальний каталог дозволяє швидко знаходити потрібні об’єкти, не вимагаючи вказань, в якому домені знаходиться об’єкт, а також використання суміжного розширеного простору імен.

1.2.2 Архітектура Active Directory

Основна структурна одиниця Active Directory – дерево доменів, пов’язаних довірчими відносинами один із одним. Усередині кожного домену може розташовуватися ієрархія організаційних одиниць (OU). Ієрархія OU усередині одного домену ніяк не пов’язана з ієрархією OU в інших доменах. Навпаки, вони повністю незалежні.

Така двоярусна ієрархічна структура надає високу степінь свободи в адмініструванні дерев доменів. Наприклад, всім деревом доменів повністю може керувати центральна служба інформаційних технологій (IT), а в усіх доменах будуть створені свої власні організаційні одиниці, де враховані як працівники, відповідальні за локальну підтримку на місцях, так і ресурси, що забезпечують цю підтримку.

У кожному окремому домені можуть бути створені додаткові OU для виконання конкретних завдань. Так в домені головного офісу – OU відділу кадрів і бухгалтерії, у філіалах – OU торгових представництв. При цьому адміністративні права для кожної із цих OU можуть делегуватися центральною службою IT співробітникам згаданих груп. І оскільки останні наділені адміністративними повноваженнями тільки в рамках своїх OU, то ніяк не зможуть перешкодити службі IT виконувати глобальне адміністрування або втрутитися в діяльність іншої OU.

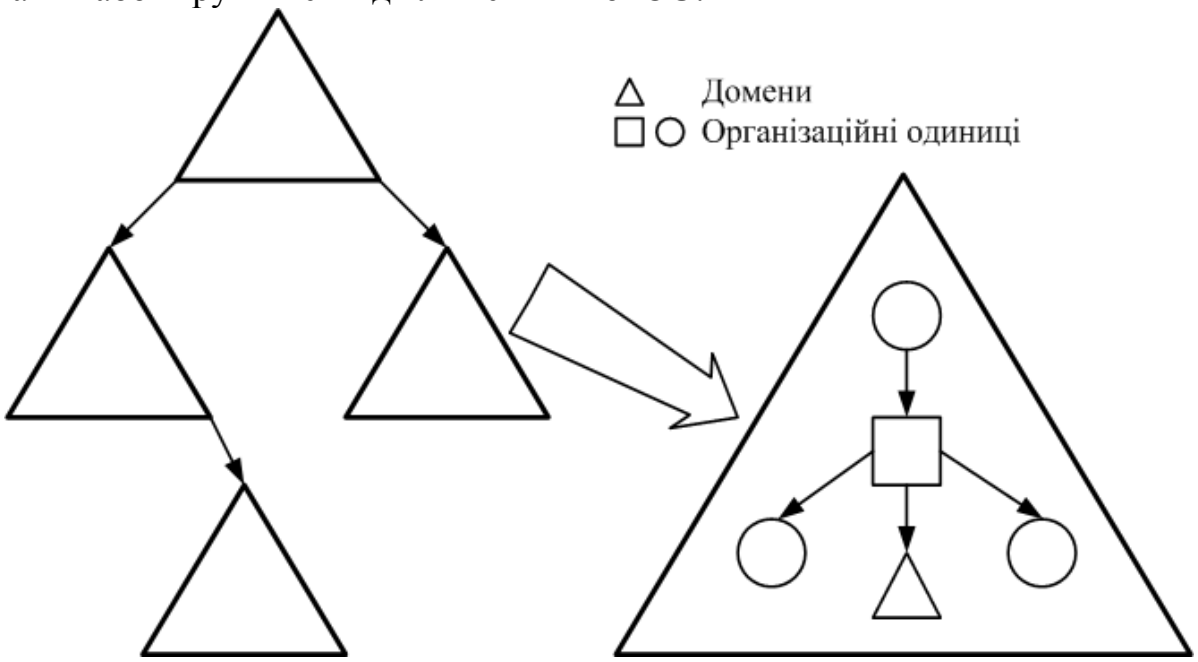

Рисунок 1.6 – Архітектура Active Directory

Така гнучкість дозволяє організувати каталог в точній відповідності із структурою організації. Причому, можливо відобразити як централізовану,

так і децентралізовану, а також деяку змішану модель управління організацією або підприємством. Наприклад, дерево доменів може бути організовано за централізованою моделлю, а OU усередині доменів – за де централізованою.

Як уже згадувалося, усередині кожного домену – своя політика безпеки. Цією політикою визначаються, зокрема, вимоги до паролів, час життя квитків Kerberos, блокування облікових записів і т.д. При створенні облікового запису в домені для нього генерується ідентифікатор безпеки (SID), частиною якого є ідентифікатор домену, що видав SID. Це можна легко визначити, якому домену належить користувач або група і які їх права доступу до ресурсів. Таким чином, можна говорити про фізичні межі безпеки домену, в рамках яких і виконується його адміністрування.

Організаційні одиниці є контейнерами, в яких можуть міститися інші організаційні одиниці або об’єкти (користувачі, групи, принтери або ресурси розподіленої файлової системи). Дозвіл створювати об’єкти або змінювати їх атрибути може бути видано окремим користувачам або групам, що дозволяє чіткіше розділяти адміністративні повноваження.

Контрольні питання до розділу 1

1. Дайте означення функцій робочої станції та сервера.
2. Обґрунтувати поняття профілю користувача.
3. Пояснити, яким чином можна забезпечити мінімальне навантаження на сервері за адміністрування мережі.
4. Основні недоліки запуску додатків з сервера.
5. Навести основні причини збереження всіх робочих файлів на дисках сервера.
6. Для чого створюється системна політика?
7. Призначення служби каталогів Active Directory.
8. Проаналізувати наслідки ініціативи нульового адміністрування.
9. Дослідити можливі варіанти розміщення даних, додатків та типів операційних систем у комп’ютерних мережах.
10. Описати недоліки та переваги різних комбінацій розміщення робочих файлів.
11. Описати використання простору імен для доменів.
12. Детально описати розділи служби каталогів Active Directory.

Розділ 2
Керування операційною системою

2.1 Система безпеки Windows 2003

Операційна система Windows NT проектувалася як ОС із зручними і надійними можливостями захисту. Одноразова реєстрація в домені Windows NT надає користувачам доступ до ресурсів всієї корпоративної мережі.

Повноцінний набір інструментів Windows NT Server полегшує адміністраторам управління системою захисту та її підтримки. Наприклад, адміністратор може контролювати коло користувачів, які мають права доступу до мережевих ресурсів: файлів, каталогів, серверів, принтерів та іншого. Права на кожний ресурс можна встановлювати централізовано.

Облікові записи користувачів також налаштовуються централізовано. За допомогою простих графічних інструментів адміністратор встановлює належність облікового запису до груп, допустимий час роботи, термін дії та інші параметри. Адміністратор має можливість аудиту усіх подій, пов'язаних із захистом доступу користувачів до файлів, каталогів, принтерів і т.д. Система також здатна блокувати обліковий запис користувача, якщо число невдалих спроб реєстрації перевищує наперед визначене значення. Адміністратори мають право встановлювати термін дії паролів, примушувати користувачів до періодичної зміни паролів і вибору паролів, що ускладнюють несанкціонований доступ.

З погляду користувача система захисту Windows NT Server повно цінна і нескладна у користуванні. Проста процедура реєстрації забезпечує доступ до ресурсів. Для користувача невидимі такі процеси, як шифрування пароля на системному рівні. (Шифрування пароля потрібне, щоб виключити передачу пароля у відкритому вигляді через мережу і перешкодити його виявленню під час несанкціонованого перегляду мережевих пакетів.) Користувач сам встановлює права доступу до тих ресурсів, якими володіє. Наприклад, щоб дозволити сумісне використання свого документа, він указує, хто і як може з ним працювати. Зрозуміло, що доступ до ресурсів підприємства контролюється тільки адміністраторами, які мають відповідні повноваження.

Ще глибший рівень безпеки реалізується для даних, які знаходяться в оперативній пам'яті комп'ютера. Доступ до них надається тільки програмам, які мають на це право. Якщо дані були видалені з диска, система запобігає несанкціонованому доступу до області диска, де вони містилися. Такий захист забороняє будь-якій програмі «переглянути» у віртуальній пам'яті машини інформацію, яка пов'язана в даний момент часу з іншим додатком.

Інтрамережі швидко стають найефективнішим способом сумісного використання інформації партнерами по бізнесу. Сьогодні доступ до закритої ділової інформації забезпечується через створення облікових записів для нових зовнішніх членів «ділового клубу». Це допомагає встановлювати довірчі відносини не тільки із співробітниками корпорації, але і з безліччю партнерів.

Віддалений доступ через відкриті мережі та зв'язок підприємств через Інтернет стимулюють постійний і швидкий розвиток технологій безпеки. Як приклад можна навести сертифікати відкритих ключів і динамічні паролі.

2.1.1 Базові відомості про шифрування

2.1.1.1 Симетричне шифрування

При симетричному шифруванні, відправник і адресат інформації користуються одним і тим самим ключем, відомим обом наперед. (Іноді такий тип називають шифруванням із загальним секретом). Зручність такої схеми є очевидною – не знаючи ключа, розшифрувати інформацію неможливо. Проте в цьому випадку виникає питання про спосіб передачі ключа адресату. Найбільш надійним, звичайно, особистий контакт, а всі інші мАють загрозу втрати або розголошення ключа.

2.1.1.2 Асиметричне шифрування

При асиметричному шифруванні початковий документ, який шифрується із використанням відкритого ключа адресата. Цей ключ може бути відомий широкому колу осіб, але прочитати зашифрований таким ключем документ зможе тільки той, у кого є парний до нього особистий (або закритий) ключ. Проблема секретної передачі ключів в даному випадку відпадає. Пари ключів генерують уповноважені системи безпеки.

2.1.1.3 Цифрові підписи

Цифрові підписи підтверджують істинність інформації, яка передається. При цьому сама інформація може бути і незашифрованою, але вважається достовірною тільки в тому випадку, якщо підписана відповідним цифровим кодом. Підпис шифрується за допомогою особистого ключа відправника, а перевіряється – за допомогою його відкритого ключа. Тут так само, як і у разі асиметричного шифрування, не потрібна секретна передача ключа.

2.1.1.4 Сертифікати

Цифрові сертифікати дозволяють побудувати надійну інфраструктуру організації. Цей спосіб захисту заснований на криптографії з відкритим ключем. Сертифікати надають клієнтам гарантії, що ті звертаються до потрібних серверів – сервери ідентифікують себе шляхом надання сертифіката. Користувач, підключаючись до сервера і одержавши від нього серти-

фікат, підписаний надійною (уповноваженою) системою, може бути упевнений, що це саме той, потрібний йому, сервер.

Сертифікати складають основу безпечної взаємодії в Інтернеті і інтрамережах. Крім високого ступеня захисту вони забезпечують одноразову реєстррацію для доступу до ресурсів інтрамереж. Користувачу не потрібно пам'ятати ім'я і пароль кожного вузла: після одноразової реєстрації програма перегляддання ресурсів надаватиме сертифікат у міру доступу до нових вузлів. В даному випадку відпадає потреба підтримувати облікову базу на кожному сервері.

У Windows 2003 вбудований сервер сертифікатів Certificate Server, який може видавати сертифікати в стандартних форматах (X.509 версій 1 і 3), а також включати розширення у міру потреби.

2.1.2 Протокол аутентифікації Kerberos

Протокол аутентифікації Kerberos визначає взаємодію між клієнтом і мережевим сервісом аутентифікації, відомим як KDC (Key Distribution Center). У Windows NT KDC використовується як сервіс аутентифікації на всіх контролерах домену. Початкова аутентифікація Kerberos інтегрована з процедурою WinLogon. Сервер Kerberos (KDC) інтегрований з існуючими службами безпеки Windows NT, що виконуються на контролері домену. Для зберігання інформації про користувачів і групи він використовує службу каталогів Active Directory.

2.1.2.1 Основи Kerberos

Kerberos є протоколом аутентифікації зі спільним секретом – і користувачу, і KDC відомий пароль. Протокол Kerberos визначає серію обмінів між клієнтами, KDC і серверами для отримання квитків Kerberos. Коли клієнт починає реєстрацію в Windows NT, постачальник функцій безпеки Kerberos одержує початковий квиток Kerberos TGT (Ticket grant ticket), заснований на зашифрованому поданні пароля. Windows NT зберігає TGT у кеші квитків на робочій станції, пов'язаній з контекстом реєстрації користувача. При спробі клієнтської програми звернутися до мережевої служби перевіряється кеш квитків: чи є в ньому правильний квиток для поточного сеансу роботи з сервером. Якщо такого квитка немає, на KDC надсилається запит з TGT для отримання сеансового квитка, що дозволить доступ до сервера.

Сеансовий квиток додається в кеш і може згодом бути використаний повторно для доступу до того ж самого сервера протягом часу дії квитка. Час дії квитка встановлюється доменними правилами і зазвичай дорівнює восьми годинам. Якщо час дії квитка закінчується в процесі сеансу, то постачальник функцій безпеки Kerberos повертає відповідну помилку, що дозволяє клієнту і серверу відновити квиток, створити новий сеансовий ключ і відновити підключення.

Сеансовий квиток Kerberos пред'являється віддаленій службі у повідомленні про початок підключення. Частини сеансового квитка зашифровані секретним ключем, який використовується спільно службою і KDC. Сервер може швидко аутентифікувати клієнта, перевіривши його сеансовий квиток, не звертаючись до сервісу аутентифікації, оскільки на сервері у кеші зберігається копія секретного ключа.

Сеансові квитки Kerberos містять унікальний сеансовий ключ, створений KDC для симетричного шифрування інформації про аутентифікацію, а також дані, які передаються від клієнта до сервера. У моделі Kerberos KDC використовується як інтерактивна довірена сторона, яка генерує сеансовий ключ.

2.1.3 Безпека і Active Directory

Розподілені служби безпеки Windows NT 5.0 використовують Active Directory як сховища облікової інформації. Зберігання облікової інформації в Active Directory означає, що користувачі і групи подані там у вигляді об'єктів каталогу. Права на читання і записування можуть бути надані окремим особам, як відносно до всього об'єкта загалом, так і відносно до окремих його властивостей. Адміністратори можуть точно задавати, хто саме уповноважений модифікувати інформацію про користувачів і яку її частину. Наприклад, оператору телефонної служби дозволяється змінювавти інформацію про телефонні номери користувачів, але при цьому він не має привілеїв системного оператора або адміністратора.

Active Directory і служби безпеки Windows NT тісно взаємопов'язані. У Active Directory зберігаються правила безпеки домену, визначено порядок використання системи (обмеження паролів, обмеження на доступ до системи та ін.). Об'єкти каталогу, які відносяться до безпеки, повинні бути захищені від несанкціонованого доступу. У Windows NT реалізована об'єктна модель безпеки і контролю за доступом до усіх об'єктів каталогу Active Directory. У кожного об'єкта є свій унікальний дескриптор захисту, який визначає права на читання або оновлення властивостей об'єкта.

Модель безпеки Windows NT забезпечує однорідний і уніфікований механізм контролю за доступом до ресурсів домену на основі членства у групах. Компоненти безпеки Windows NT довіряють інформації, що зберігається в каталозі захисту. Наприклад, сервіс аутентифікації Windows NT зберігає зашифровані паролі користувачів у безпечній частині каталогу об'єктів користувача. За замовчуванням операційна система «вважає», що правила безпеки захищені і не можуть бути змінені будь-ким несанкціоновано. Загальна політика безпеки домену також зберігається в каталозі Active Directory.

2.1.4 Довірчі відносини між доменами

У Windows 2003 домени можуть бути організовані у вигляді ієрархічних дерев. Між доменами встановлюються довірчі відносини. Підтримуються два види таких відносин:

– явні однонаправлені довірчі відносини з доменами Windows NT 4.0;

– двосторонні транзитивні довірчі відносини між всіма доменами, які входять у дерево.

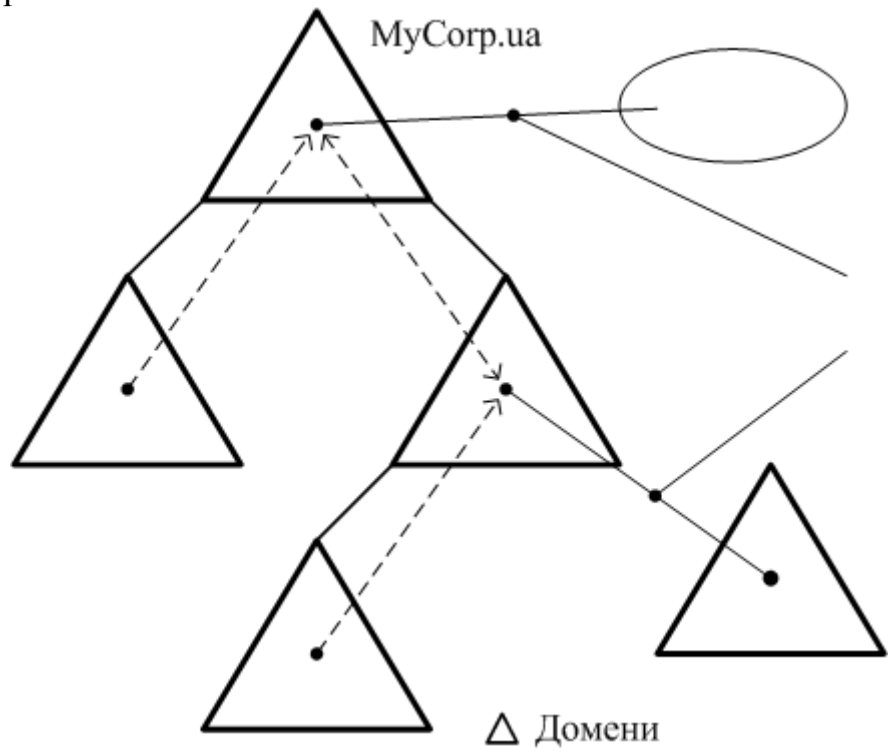

Рисунок 2.1 – Довірчі відносини між доменами

Явні довірчі відносини встановлюються не тільки з доменами старого типу, але і у тому випадку, коли неявні двосторонні відносини непридатні для використання: наприклад, для домену фінансового відділу або бух галтерії. Встановлення явних односторонніх довірчих відносин автоматично відміняє неявні довірчі відносини Kerberos. Неявні двосторонні довірчі відносини значно полегшують управління обліковими записами з декількох доменів, оскільки усі домени в дереві неявно довіряють один одному.

2.1.5 Елементи безпеки системи

2.1.5.1 Облікові записи користувачів і груп

Будь-який користувач Windows NT характеризується певним обліковим записом. Під обліковим записом розуміється сукупність прав і додаткових параметрів, які асоціюються з певним користувачем. Крім того, користувач належить до однієї або декількох груп. Приналежність до групи дозволяє швидко і ефективно призначати права доступу і повноваження.

Є декілька вбудованих облікових записів користувачів і груп. Ці облікові записи наділені певними повноваженнями і можуть використовуватися як основа для нових облікових записів.

До вбудованих облікових записів користувачів відносяться:

- *Guest* – обліковий запис, що фіксує мінімальні привілеї гостя;
- *Administrator* – вбудований обліковий запис для користувачів, наділених максимальними привілеями;
- *Krbtgt* – вбудований обліковий запис, використовуваний при початковій аутентифікації Kerberos.

Окрім них є два прихованих вбудованих облікових записи:

- *System* – обліковий запис, використовуваний операційною системою;
- *Creator owner* – власник (файлу або каталогу).

Назвемо вбудовані групи:

- локальні
  - *Account operators* – оператори облікових записів;
  - *Administrators* – адміністратори;
  - *Backup operators* – оператори резервного копіювання;
  - *Guests* – гості;
  - *Print operators* – оператори сервісу друку;
  - *Replicator* – клієнти служби реплікації;
  - *Server operators* – оператори сервера;
  - *Users* – користувачі;
- глобальні
  - *Domain guests* – гості домену;
  - *Domain Users* – користувачі домену;
  - *Domain Admins* – адміністратори домену;
  - *Domain Computers* – всі комп'ютери домену;
  - *Domain Controllers* – всі контролери домену;
- універсальні
  - *Enterprise Admins* – адміністратори підприємства;
  - *Schema Admins* – адміністратори схеми.

Крім цих вбудованих груп є ще ряд спеціальних груп:

- *Everyone* – в цю групу за замовчуванням включаються взагалі всі користувачі в системі;
- *Authenticated users* – в цю групу включаються тільки аутентифіковані користувачі домену;
- *Self* – сам об’єкт.

Для переглядання облікових записів використовується зліпок консолі управління *Directory Service Manager,* у якому треба вибрати контейнер *Users.* Для перегляду і модифікації властивостей облікового запису досить вибрати ім’я користувача або групи і на екрані з’явиться діалогове вікно *User Properties.*

Діалогове вікно містить такі вкладки:

- *General* – загальний опис користувача; всі параметри необов'язкові;
- *Address* – домашня і робоча адреса користувача; всі параметри необов'язкові;
- *Account* – обов'язкові параметри облікового запису;
- *Telephone/notes* – необов'язкові параметри;
- *Organization* – додаткові необов'язкові відомості;
- *Member Of* – обов'язкова інформація про приналежність користувача до груп;
- *Dial-in* – параметри віддаленого доступу;
- *Object* – ідентифікаційні відомості про призначений для користувача об'єкт;
- *Security* – інформація про захист об'єкта.

Необов'язкові параметри можна і не вводити, але вони корисні при пошуку того або іншого користувача за другорядними ознаками.

Вікно властивостей облікового запису користувача (вкладка *Account)* дозволяє вказати:

– характеристики пароля (чи повинен користувач його змінити при наступному вході в домен, чи має пароль обмеження за терміном);
– чи не заблокований обліковий запис;
– термін закінчення часу дії облікового запису;
– профіль користувача і його домашній каталог;
– дозволений час роботи;
– робочі станції, з яких дозволено реєстрацію в домені.

Для включення (виключення) користувача в ту чи іншу групу використовується вкладка *Membership.* Щоб включити користувача в нову групу, необхідно виділити її у списку і натиснути кнопку *Add.* Щоб виключити користувача із групи, необхідно виділити його у списку і натиснути кнопку *Remove.*

Права доступу до об'єкта стануть доступні для перегляду і редагування, якщо вибрати вкладку *Security.* Якщо даний об'єкт не є контейнером, то для нього визначаються найбільш загальні дозволи, наведені в таблиці 2.1.

Доступ можна не тільки надавати (поле *Allow),* але і забороняти (поле *Deny).* Це дозволяє уникнути створення безлічі додаткових груп з наборами прав доступу, які небагато чим відрізняються одна від одної.

Щоб додати нового користувача в організаційну одиницю (OU), необхідно натиснути на її імені правою кнопкою миші і вибрати в контекстному меню команду *New/User.* Після цього з'явиться діалогове вікно *Create User.* У ньому так само можна вказати загальне ім'я користувача (cn), його повне ім'я, пароль (з терміном дії, якщо є) чи вказати про заборону використання цього облікового запису.

Таблиця 2.1 – Права доступу до об’єкта

Право доступу	**Опис**	**Облікові записи, яким право доступу надане за замовчуванням**
Full Control	Повний доступ	*Administrators, Account operators, System*
Read	Читання	*Administrators, Account operators, System, Authenticated users, Self*
Write	Записування	*Administrators, Account operators, System*
Send As	Відправити як	*Administrators, Account operators, System, Self.*
Receive as	Прийняти як	*Administrators, Account operators, System, Self.*
Change password	Змінювати пароль	*Administrators, Account operators, System, Self, Everyone*.

Властивості груп можна переглянути так само, як і властивості будь-якого об’єкта у каталозі: натиснути правою кнопкою миші ім’я групи і в контекстному меню вибрати команду *Properties*. Після цього з’явиться діалогове вікно *Group Properties*.

У діалоговому вікні *Group Properties* є вкладки з такою інформацією:

- *General* – загальною про групу, а також список її членів;
- *Membership* – про те, до яких груп входить вибрана група;
- *Managed by* – про адміністратора групи;
- *Object* – про об’єкт-групу;
- *Security* – про права доступу до об'єкта-групи.

Список членів групи подано у вигляді відносного імені користувачів у каталозі, наприклад, domain/Users/Account Name. Для додавання нових користувачів треба натиснути кнопку *Add* і вибрати користувачів цього або іншого домену.

Щоб включити існуючу групу в іншу, треба у вікні властивостей групи вибрати вкладку *Membership.* Після цього з’явиться список груп, у які входить вибрана. Оскільки в загальному випадку групи можуть належати різним доменам, імена груп подані у вигляді відносного імені об’єкта у каталозі, наприклад, domain/Builin/Administrators. Для включення групи в ще одну групу натискають кнопку *Add* і вказують потрібну групу. Для виключення вибраної групи з іншої – виділяють у списку ім’я тієї групи, яку треба покинути, і натискають кнопку *Remove.*

Додання нової групи виконується майже так само, як і додання нового користувача. Різниця лише у тому, що, додаючи групу спочатку вказується тільки ім’я об’єкта.

2.1.5.2 Локальна політика безпеки

Для редагування локальної політики безпеки необхідно в діалоговому вікні *Domain Properties,* на вкладці *General* натиснути кнопку *Edit* в групі *Computer security policy* при включеному прапорці *Use a local policy object in this domain.* На екрані з’явиться діалогове вікно *Default Local Policy Properties.*

Локальна політика безпеки регламентує правила безпеки на локальному комп'ютері. З її допомогою можна розподілити адміністративні ролі, конкретизувати привілеї користувачів, призначити правила аудиту.

Вкладка *Administrative Roles* відображає делегування адміністративних повноважень. Припустимо, що адміністратору необхідно надати повноваження оператора облікових записів користувачу Zahar, розташованому в OU=VSTU у домені O=Vinnica. Для цього вибирають у списку вбудованих адміністративних ролей *Account operators* і натискають кнопку *Add.* Із списку всіх користувачів і груп вибирають необхідного користувача (Vinnica/VSTU/Zahar).

За допомогою вкладки *User Rights* можна наділяти окремих користувачів певними додатковими повноваженнями.

Обираючи привілеї, можна побачити список користувачів, яким вони надані, а натиснувши кнопку Add – можна додати у цей список нові облікові записи. У таблиці 2.2 вказано деякі вбудовані привілеї і облікові записи користувачів, які мають їх за замовчуванням.

Таблиця 2.2 – Привілеї які надані користувачам за замовчуванням

Привілей	**Опис**	**Облікові записи, яким привілей наданий за замовчуванням**
Backup files and directories	Виконувати резервне копіювання файлів і каталогів (пріоритет над правами доступу до файлів і каталогів)	*Administrators, Backup operators*
Load and unload device drivers	Встановлювати і видаляти драйвери пристроїв	*Administrators*
Shutdown the system remotely	Виконувати виключення системи віддалено	*Administrators*
Restore files and directories	Відновлювати файли і каталоги з резервної копії	*Administrators, Backup operators*
Manage auditing and security log	Указувати, які типи доступу до ресурсів підлягають реєстрації, а також переглядати і очищати журнал аудиту	*Administrators*
Shutdown the system	Вимикати систему	*Administrators, Backup operators*
Change the system time	Встановлювати внутрішній таймер комп'ютера	*Administrators*
Take ownership on files or other objects	Вступати у володіння файлами, каталогами, принтерами та іншими об'єктами	*Administrators*
Log on locally	Реєструватися локально з клавіатури комп'ютера	*Administrators, Backup operators*
Access this computer from the network	Підключатися до комп'ютера через мережу	*Administrators, Everyone*

2.1.5.3 Доменна політика

Доменна політика встановлює правила для всіх облікових записів в домені, об'єднуючи такі сфери, як правила паролів, блокування облікових записів і т.д.

Для редагування доменної політики слід натиснути кнопку *Edit* в групі *Domain security policy* на вкладці *General* діалогового вікна *Domain Properties*. На екрані з'явиться діалогове вікно *Default Domain Policy Properties*. З його допомогою можна змінювати:

- максимальний термін дії пароля;
- мінімальну довжину пароля;
- мінімальний термін незмінності пароля;
- унікальність пароля;
- блокування облікових записів при невдалій реєстрації;
- тривалість блокування;
- а також деякі інші параметри.

Якщо пароль користувача довгий час є незмінним, то захищеність системи від несанкціонованого доступу значно знижується. Саме тому система повинна примушувати користувача до періодичної зміни пароля. Політика ведення облікових записів дозволяє задати певний термін дії пароля в межах від 1 до 999 днів або призначити пароль постійним. За замовчуванням тривалість дії пароля 42 дні.

Якщо адміністратор задав параметр *Password never expires* для конкретного користувача, той може не змінювати пароль. Але така практика рекомендується тільки для службових облікових записів, від імені яких виконуються сервіси в системі.

За замовчуванням довжина пароля користувача знаходиться у межах від 0 до 14 символів. Зрозуміло, що при підвищених вимогах до захищеності системи порожній пароль недопустимий. В цьому випадку адміністратор системи призначає мінімальну довжину пароля. Створюючи новий обліковий запис для користувача, адміністратор може вказати пароль довільної довжини, незалежно від обмеження, заданого політикою ведення облікових записів. Проте якщо пароль змінюється користувачем після реєстрації в системі, то параметри нового пароля повинні точно відповідати політиці ведення облікових записів.

Обмеження на мінімально можливий термін зміни пароля користувачем доцільно, наприклад, якщо в системі працює багато користувачів-новачків. По-перше, певний термін дає користувачам, які недавно познайомилися з Windows NT, можливість звикнути до особливостей захищеної роботи і переконатися в необхідності пам'ятати свій пароль. А будь-кому, хто забув свій пароль, зможе допомогти адміністратор.

По-друге, користувач-початківець, змінивши після закінчення терміну дії пароль, може захотіти повернутися до колишнього. Але зробити це і погіршити таким чином захищеність системи не дозволить примусова за-

тримка. Це особливо ефективно, якщо встановити параметр відстеження унікальності пароля.

Мінімальна затримка дозволу на зміну пароля визначається у межах від 1 до 999 днів. За замовчуванням вона не обмежується. Зазвичай, досить встановити 14 днів.

Параметр *Password uniquiness* дозволяє запам'ятовувати в системі від 1 до 24 паролів, що забезпечує унікальні паролі для користувача впродовж тривалого часу.

Включивши прапорець *Password must be strong* адміністратору більше не доведеться роз'яснювати користувачам, чому як пароль не можна використовувати своє ім'я, імена дружини, дітей, інших родичів і домашніх тварин, дату свого дня народження і взагалі будь-які слова і фрази, присудні в словниках. Система сама буде клопотати про те, щоб пароль містив як мінімум три з перерахованих нижче типів символів:

- прописні букви латинського алфавіту;
- рядкові букви латинського алфавіту;
- цифри;
- спеціальні символи.

Якщо включено прапорець *User must logon in order to change Password,* користувачу доведеться, перш ніж змінити пароль, реєструватися в системі. Інакше він зробить це і без реєстрації. Регулювання цього параметра особливо актуальне, коли закінчується термін дії пароля. Якщо прапорець включено, користувач самостійно не змінить пароль, і йому доведеться звернутися до адміністратора. Якщо прапорець виключено, то пароль можна змінити, не повідомляючи адміністратора.

Вкладка *Account Lockout* діалогового вікна *Default Domain Policy Properties* дозволяє захистити систему від «словникових атак» – програм, що зламують систему захисту шляхом перебору найчастіше використовуваних слів і фраз із словника для пошуку пароля. Щоб така програма не могла працювати, необхідно встановити максимальне число невдалих спроб реєстрації (за замовчуванням п'ять), після яких обліковий запис буде заблокований. Можна також вказати час, через який лічильник невдалих спроб «обнулиться» (за замовчуванням 20 хвилин), і час, протягом якого обліковий запис буде блокований (за замовчуванням 1 година). Після вдалої реєстрації лічильник невдалих реєстрацій буде «обнулено».

2.1.5.4 Редактор конфігурацій безпеки

При автоматичному установленні операційних систем на велике число комп'ютерів, під час адміністрування великих корпоративних мереж всі розглянуті інструменти, не дивлячись на свою корисність, є недостатньо ефективними, що в цілому призводить до підвищення вартості адміністрування. Для роботи в таких умовах необхідний принципово інший метод, об'єднуючий у собі можливості всіх згаданих інструментів. Тільки так мо-

жна гарантувати ефективну політику безпеки і контроль захисту в масштабах великого підприємства. В ролі такого інструменту успішно виступає редактор конфігурацій безпеки. Питання, пов'язані із безпекою, можна умовно розділити на декілька областей.

За замовчуванням підтримуються такі області безпеки:

– політика безпеки – завдання різних атрибутів безпеки на локальному і доменному рівнях; так само охоплює деякі установлення на машинному рівні;

– управління групами з обмеженнями – дозволяє управляти членством в групах, які, на думку адміністратора, «чутливі» з погляду безпеки системи;

– управління правами і привілеями – дозволяє редагувати список користувачів і їх специфічних прав і привілеїв;

– дерева об'єктів – включають три області захисту: об'єкти каталогу Active Directory, ключі реєстру, локальну файлову систему; для кожного об'єкта в дереві шаблони безпеки дозволяють конфігурувати і аналізувати характеристики дескрипторів захисту, включаючи власників об'єкта, списки контролю доступу і параметри аудиту;

– системні служби (мережеві або локальні) – побудовані відповідним чином дають можливість незалежним виробникам програмного забезпечення розширювати редактор конфігурацій безпеки для усунення специфічних проблем.

2.1.5.5 Функції редактора конфігурацій безпеки

Редактор конфігурацій безпеки – зліпок консолі управління MMC (Microsoft Management Console). Розглянемо його основні функції.

Визначення шаблонів конфігурацій безпеки. Для реалізації безпеки в масштабах підприємства, що налічує сотні або тисячі комп'ютерів, краще всього скористатися шаблонами замість індивідуального настроювання кожної машини. Припустимо, що всі комп'ютери можуть мати десять різних варіантів настроювання параметрів захисту. У такому разі зручно зробити десять шаблонів, кожний з яких відповідатиме своєму варіанту захисту, і застосовувати ці шаблони відповідно до потреб. В процесі застосування шаблону в реєстр комп'ютера вносяться зміни, які і визначають настроювання системи безпеки. Шаблони безпеки в Windows NT – це текстові файли, формат яких схожий на формат inf-файлів. У окремих секціях описуються різні параметри безпеки. При завантаженні файлу в редактор конфігурацій ці параметри відображаються в зручному для аналізу і редагування вигляді. Редактор також дозволяє створювати нові файли-шаблони.

2.2 Контроль реєстру робочої станції

Системний реєстр є центральним сховищем даних про конфігурацію в операційних системах Windows, і здійснення контролю над ним є однією з

найважливіших частин роботи системного адміністратора. Можливість одержання доступу до реєстру робочої станції як у віддаленому, так і в автоматизованому режимі, дозволить контролювати практично будь-який аспект функціональності системи, а також захищати сам реєстр від ушкодження через неавторизовані зміни.

2.2.1 Використання системних політик

Усі операційні системи Windows включають можливість проведення системної політики (system policy), варіанти якої дозволяють здійснювати значний обсяг контролю над конфігурацією робочої станції. Визначивши набір правил системної політики і впровадивши його, можна контролювавти, до яких саме компонентів операційної системи буде дозволений доступ користувачів, які додатки ці користувачі зможуть запускати, а також який вигляд буде мати їх робочий стіл. Правила системної політики – це набір установлень системного реєстру, що упаковані у файл системної політики і зберігаються на диску сервера. Коли користувач підключається до мережі, робоча станція завантажує файл системної політики із сервера і застосовує зафіксовані там установлення до свого системного реєстру. Оскільки робоча станція завантажує файл системної політики автоматично під час процесу входу користувача в мережу, а самі користувачі ніяк не можуть цього уникнути, то це робить системну політику засобом обмеження доступу користувачів до інтерфейсу Windows.

Застосування різних правил системної політики є альтернативою прямій зміні ключів системного реєстру і тим самим зменшує можливість неправильного функціонування системи внаслідок орфографічних та інших помилок. Замість того, щоб вручну переглядати вміст дерева реєстру в пошуках незрозумілих ключів і імен елементів, а потім вводити закодовані значення, можна просто створити файл системної політики за допомогою утиліти з графічним інтерфейсом за назвою System Policy Editor (SPE, Редактор системної політики). SPE демонструє установлення реєстру у вигляді різних правил політики, що є звичайними фразами англійською мовою зі стандартними елементами діалогових вікон Windows, що розташовані у вигляді ієрархічної деревоподібної структури.

2.2.2 Шаблони системної політики

Редактор системної політики – це просто інструмент для створення файлів системної політики, він зовсім не контролює конкретні варіанти політики, що створює. Самі правила системної політики беруть початок із шаблонів системної політики, що є файлами формату ASCII, які містять ключі реєстру, можливі значення, пояснювальний текст. Усе це формує правила політики, які відображаються в редакторі системної політики.

Наприклад, фрагмент шаблона системної політики Common.adm створює варіант політики за назвою Remote update, показаний таким чином:

```
CATEGORY !!Network CATEGORY !!Update
    POLICY !!RemoteUpdate
    KEYNAME System\CurrentControlSet\Control\Update ACTIONLISTOFF
    . VALUENAME "UpdateMode" VALUE NUMERIC 0
    END ACTIONLISTOFF
    PART !!UpdateMode                          DROPDOWNLIST REQUIRED
    VALUENAME "UpdateMode" ITEMLIST
    NAME ! !UM_Automatic VALUE NUMERIC 1
    NAME !!UM_Manual                           VALUE NUMERIC 2
    END ITEMLIST END PART PART !!UM_Manual_Path EDITTEXT
        VALUENAME "NetWorkPath"
    END PART
    PART !!Display Errors                      CHECKBOX
        VALUENAME "Verbose" END PART PART !!LoadBallance
        VALUENAME "LoadBallance" END PART END POLICY
        END CATEGORY ; Udate END CATEGORY ; Network
```

Всі операційні системи Windows включають крім SPE безліч файлів шаблонів системної політики. До основних шаблонів можна віднести файл Windows.adm, який включає шаблони варіантів політики Windows, а також файл Common.adm, який містить шаблони варіантів політики, застосовних як у Windows. Інші додатки, наприклад, Microsoft Office чи Internet Explorer, мають власні набори файлів шаблонів, які містять політики, специфічні для даних додатків. Крім того, можна самостійно створювати свої шаблони для зміни інших установень реєстру.

Вибравши в меню Options (Параметри) команду Policy Template (Шаблон), можна завантажити шаблони, які SPE буде використовувати для створення файлів політики. Існує можливість завантажувати велику кількість шаблонів в SPE, і політики, що містяться в них, будуть сполучатися з інтерфейсом програми. При запуску SPE завантажує ті шаблони, що були застосовані під час останнього завершення ОС, за умови, що відповідні файли як і раніше знаходяться на тих самих місцях.

Якщо в SPE використовується безліч шаблонів системної політики, ймовірна ситуація, коли політики, обумовлені двома різними шаблонами, конфігурують ті ж налаштування системного реєстру. Якщо відбувається подвоєння подібного типу, варіант політики, розташований ближче до кореня ієрархії діалогового вікна Properties (Властивості) об’єкта, має перевагу.

2.2.3 Файли системної політики

За допомогою SPE можна створювати політики, що застосовуються тільки до конкретних користувачів чи груп комп’ютерів, а також політики для користувача за замовчуванням (Default User) і комп’ютера за замовчуванням (Default Computer). Політики для численних користувачів мережі і комп’ютерів зберігаються в єдиному файлі, який кожен комп’ютер завантажує із сервера в процесі підключення до мережі. Файл системної політики для операційної системи Windows називається Ntconfig.pol. Всі опера-

ційні системи Windows мають власні версії утиліти, System Policy Editor, але усі версії мають однаковий інтерфейс.

Версії SPE операційних систем Windows за замовчуванням встановлюються разом із самими операційними системами, і їх можна запускати в будь-якій системі з Windows, скопіювавши файли на диск іншого комп'ютера. Однак тип файлів системної політики, які створюються SPE, залежить від тієї операційної системи, у якій працює програма. Можна створювати файли політики Windows 98, запускаючи SPE на машині з операційною системою Windows 98, але не вдасться сформувати файл системної політики Windows 98 на машині з Windows XP і навпаки.

2.2.3.1 Створення файлів політики

Процес створення нового файлу політики зводиться до запуску SPE і вибору в меню File (Файл) команди New Policy (Створити). За замовчуванням програма створює об'єкти Default User і Default Computer. Відкривши об'єкт, можна побачити правила політики, що можуть бути для нього сконфігуровані. Правила політики, що створюються в рамках об'єктів за замовчуванням, відбиваються на всіх робочих станціях, що підключаються до мережі. Також є можливість формування додаткових об'єктів користувачів і об'єктів груп, що співвідносяться, відповідно, з NetBIOS-ім'ям комп'ютерів та ім'ям облікових записів груп у домені Windows. Правила політики для комп'ютерів модифікують установлення реєстру в ключі HKEY_LOCAL_MACHINE, в той час як правила для користувачів і груп вносять зміни в ключ реєстру HKEY_CURRENT_USER. Коли створюється новий об'єкт користувача чи комп'ютера групи, SPE копіює в нього вміст відповідного об'єкта за замовчуванням і створює нову піктограму. З цими інструментами можна реалізувати різні варіанти політики для різних типів користувачів мережі.

Робочі станції завжди автоматично перевіряють наявність файлу політики під час підключення до мережі, і якщо такий файл там присутній, завантажують і обробляють його. Файли системної політики завжди обробляються вже після завантаження профілів користувачів, тому установлення реєстру у файлі системної політики мають переваги перед установленнями куща реєстру з профілю користувача.

2.2.3.2 Пріоритети політики

Задача створення стратегії системної політики, яка надає достатній контроль над робочими станціями мережі і яку одночасно досить просто підтримувати, цілком залежить від адміністратора мережі. Як і у випадку більшості адміністративних задач, зручніше реалізовувати системну політику стосовно груп користувачів, ніж створювати індивідуальні варіанти політики для кожного користувача. Формуючи файл групової політики в SPE, існує можливість задання пріоритету для кожної групи (вибравши в

меню Options (Параметри) команду Group Priority (Пріоритет групи)), що контролює порядок, у якому варіанти політики будуть застосовуватися до системи. Коли робоча станція обробляє файл системної політики і користувач є членом більш ніж однієї групи, система застосовує групові політики в порядку їхніх пріоритетів: від найнижчого до найвищого. Таким чином, політики з високим пріоритетом можуть змінити установлення політик з більш низьким рівнем пріоритету.

Коли в редакторі системної політики створюється об'єкт індивідуального комп'ютера, він має вищий рівень пріоритету, ніж відповідний об'єкт за замовчуванням (Default Computer). Коли користувач проходить реєстрацію на робочій станції, що є об'єктом для комп'ютера, система обробляє політики для індивідуального комп'ютера й ігнорує політики об'єкта Default Computer. Аналогічно, якщо користувач є індивідуальним об'єктом, система завантажує індивідуальні політики для даного користувача й ігнорує усі політики для груп, до яких цей користувач належить, як і політики для користувача за замовчуванням (Default User). Політики для користувачів і груп мають також перевагу над політиками для комп'ютерів у тих випадках, коли порушуються кілька ключів реєстру, її існування можливе як у HKEY_LOCAL_MACHINE, так і у HKEY_CURRENT_USER. Якщо установлення присутнє в обох ключах, перевага є на боці значення, розташованого в ключі реєстру HKEY_CURRENT_USER.

Системні політики застосовуються до всіх користувачів, включаючи і тих, хто має адміністративний доступ.

2.2.4 Визначення правил політики

Після завантаження шаблона політики в SPE і створення нового файлу системної політики можна починати створення нових об'єктів і конфігурувати їх правила політики. Об'єкт кожного комп'ютера чи користувача групи у файлі політики містить ієрархію категорій, що має різні варіанти правил політики. Кожне правило з'являється у вигляді окремого пункту, що може набувати одного з трьох наступних значень, які мають відношення до реалізації даної політики.

- *Enabled* (Дозволено). Застосовує правило політики до системного реєстру з використанням зазначеного значення.
- *Disabled* (Заборонено). Не застосовує правило політики до реєстру та видаляє його з реєстру, якщо воно там уже присутнє.
- *Undefined* (Не визначено). Ігнорує правило політики, не змінюючи реєстр, незалежно від того, є присутньою там дана політика чи ні.

Крім цього пункту правило політики може мати ще цілий ряд інших керуючих елементів, асоційованих з ним, що показуються в області Settings (Параметри) у нижній частині діалогового вікна, якщо правило дозволене. Ці керуючі елементи можуть набувати декількох форм, включаючи додаткові пункти, поля для введення даних і перемикачі. Спосіб зміни

реєстру цими елементами керування залежить від вимог окремих установок і структури шаблона політики. Деякі правила політики просто створюють елемент реєстру із певним ім'ям, у той час як інші можуть призначати конкретній установці буквено-цифрове чи шістнадцяткове значення.

2.2.5 Обмеження діяльності робочої станції за допомогою системної політики

Одна з основних функцій системної політики полягає в тому, щоб заборонити доступ користувачів до певних елементів операційної системи. Для цього існує кілька причин, наприклад:

– не допускати запуск користувачами неавторизованого програмного забезпечення;

– не допускати зміни користувачами елементів оформлення;

– ізолювати користувачів від можливостей, якими вони не зможуть безпечно скористатися.

Здійснивши зазначені заходи, можна перешкодити тому, щоб користувачі витрачали багато часу на непродуктивну діяльність, яка часто призводить до порушень функціонування робочих станцій внаслідок бездумних експериментів, для усунення наслідків яких часто потрібно потужна тех.-нічна підтримка. Наступні пункти описують як саме можна застосовувати визначені правила системної політики для керування конфігурацією робочої станції.

2.2.5.1 Обмеження додатків

Однією з головних причин нестабільності робочих станцій Windows є установлення несумісних додатків. Більшість пакетів програмного забезпечення для Windows включають модулі бібліотек, що динамічно підключаються, які встановлюються в системні каталоги Windows. Дуже часто такі модулі замінюють вже існуючі, будучи їхніми новішими версіями, розробленими для підтримки додатка. Проблема даного типу програмного забезпечення полягає в тому, що установлення нового додатка з заміною визначеної DLL-бібліотеки на новішу версію цілком може порушити функціонування вже існуючого додатка в системі.

Один зі способів, що дозволяє уникнути подібних складнощів, які виникають через даний тип конфлікту версій, полягає в підборі групи додатків, яка задовольняє групу користувачів, і наступного ретельного тестування всіх додатків цієї групи одночасно. Як тільки стане зрозуміло, що додатки сумісні, їх варто установити на робочі станції і заборонити користувачам додання іншого програмного забезпечення, яке зможе додати несумісні елементи. Обмеження програмного забезпечення робочих станцій також не дозволить користувачам установлювати такі непродуктивні додатки як ігри, що віднімають величезну кількість часу, дискового простору і навіть пропускної здатності мережі.

Є кілька технічних прийомів, які можна використовувати для запобігання установлення користувачами неавторизованого програмного забезпечення на свої робочі станції. Один з них є методом грубої сили і полягає в тому, щоб заборонити користувачам доступ до носія, з якого вони могли б установити шкідливу програму. Встановлюючи комп'ютери без DVD-приводів, можна ліквідувати первинне джерело неавторизованого програмного забезпечення. Також можливо запобігати доступу до дисковода за допомогою запуску спеціальної програми, наприклад, сервісу FloppyLocker, включеного в Microsoft Zero Administration Kit.

Третім потенційним джерелом неавторизованих програм є Інтернет. Якщо планується надати користувачам доступ до таких сервісів як Web, то при цьому слід не допустити установлення користувачами програм, завантажених з Інтернету. Один зі способів домогтися цього, а також уникнути будь-якого установлення неліцензійного програмного забезпечення, полягає у використанні правил системної політики, що не дозволяють користувачам запускати програми установлення, необхідні для інсталяції програмного забезпечення. У вирішенні даного питання можуть допомогти правила політики, перераховані нижче.

- *Remove Run Command from Start menu* (Видалити команду Виконати з меню кнопки Пуск). Не дозволяє користувачу запускати програму установлення додатка, забороняючи доступ у діалогове вікно Run (Виконати).
- *Run Only Allowed Windows Applications* (Запускати тільки дозволені додатки Windows). Дозволяє адміністратору визначити список виконуваних файлів, які є єдиними програмами, що можна запускати користувачу. Використовуючи дану політику, треба не забути включити до списку усі виконувані файли, необхідні для нормальної роботи Windows, наприклад, Systray.exe чи Explorer.exe.
- *Disable MS-DOS Prompt* (Заборонити режим MS-DOS). Не дає можливість користувачам Windows запускати програми в режимі емулювання MS-DOS.

2.2.5.2 Блокування інтерфейсу

Існує досить багато елементів інтерфейсу Windows, доступ до яких недосвідчених користувачів не є обов'язковим. Тому їхнє блокування допоможе найбільш зацікавленим користувачам утриматися від дослідження речей, яких вони до кінця не розуміють, і ліквідує ризик ушкодження системи в ході цього пізнавального процесу. Деякі політики, за допомогою яких це можна зробити, перераховані нижче.

- *Remove Folders from Settings on Start menu* (Видалити папки з меню кнопки Пуск). Блокується поява папок Control Panel (Панель керування) і Printers (Принтери) у групі Settings (Настроювання) меню кнопки Start (Пуск). Дане правило політики не перешкоджає доступу користувачів до панелі керування іншими способами, але робить менш ймовірним проник-

нення туди користувача з цікавості. Можна також блокувати певні піктограми панелі керування системи Windows, використовуючи такі правила політики:

– *Restrict Network Control Panel* (Обмеження для програми настроювання мережі);

– *Restrict Printer Settings* (Обмеження для програми настроювання принтерів);

– *Restrict Passwords Control Panel* (Обмеження для програми настроювання захисту);

– *Restrict System Control Panel* (Обмеження для програми настроювання системи).

- *Remove Taskbar from Settings on Start menu* (Видалити панель задач з меню кнопки Пуск). Не дозволяє користувачам змінювати конфігураційні установлення панелі задач і меню кнопки Start (Пуск).
- *Remove Run Command from Start menu* (Видалити команду Виконати з меню кнопки Пуск). Не дає можливість користувачам запускати програми чи виконувати команди за допомогою діалогового вікна Виконати. Ця політика також забезпечує додаткову ізоляцію користувачів від таких елементів, як панель керування чи командний рядок, до обох можна одержати доступ за допомогою команд діалогового вікна Виконати.
- *Hide All Items on Desktop* (Сховати всі піктограми робочого столу). Блокується поява всіх піктограм робочого столу Windows. Якщо є бажання, щоб користувачі при запуску програм спиралися на меню кнопки Start (Пуск), можна використовувати це правило політики для видалення піктограм робочого столу, що відволікають увагу.
- *Disable Registry Editing Tools* (Заборонити редагування реєстру). Прямий доступ до системного реєстру Windows повинен бути обмежений для усіх, крім кваліфікованих користувачів. Політика не дозволяє звичайним користувачам запускати утиліти редагування реєстру, що входять до складу операційних систем.
- *Disable Context Menus for the Taskbar* (Заборонити контекстні меню для панелі задач). Не дозволяє системі демонструвати контекстні меню, що з'являються при натисненні правою кнопкою миші на піктограмі панелі задач.

Також можна використовувати системну політику для захисту оформлення елементів інтерфейсу, що дозволяє користувачам не гаяти час на настроювання кольорової схеми екрану і шпалер робочого столу. Крім того, можна самостійно сконфігурувати ці параметри, створивши стандарти зованій робочий стіл для всіх робочих станцій мережі. Ці політики перераховані нижче.

- *Deny Access to Display Icon* (Заборонити можливість настроювання екрану). Видаляє піктограму Display (Екран) з вікна Control Panel (Панель керування), не дозволяючи користувачам одержувати доступ до конфігураційних настроювань екрану.

- *Hide Background Tab* (Сховати вкладку вибору фону). Блокує вкладку Background (Фон) діалогового вікна Display Properties (Властивості екрану).
- *Hide Screen Saver Tab* (Сховати вкладку вибору заставки). Блокує вкладку Screen Saver (Заставка) діалогового вікна Display Properties (Властивості екрану).
- *Hide Appearance Tab* (Сховати вкладку вибору оформлення). Блокує вкладку Appearance (Оформлення) діалогового вікна Display Properties (Властивості екрану).
- *Hide Settings Tab* (Сховати вкладку установлення параметрів). Блокує вкладку Settings (Параметри) діалогового вікна Display Properties (Властивості екрана).
- *Wallpaper Name* (Фоновий малюнок). Дозволяє задавати шлях і ім'я файлу растрового зображення, яке буде використовуватися як фоновий малюнок робочого столу.
- *Color Scheme* (Кольорова схема). Дозволяє задаватити таке оформлення, яке система повинна буде використовувати для усіх елементів робочого столу.

Як альтернативу профілям користувачів системна політика надає можливість більш точної конфігурації ярликів, які є на робочому столі Windows і в меню кнопки Start (Пуск). Замість звертання до профілю користувача за допомогою даних правил політики можна вказати розташування індивідуальних папок, які містять ярлики для різних елементів інтерфейсу. Використовуються такі правила політики:

- *Custom Programs Folder/Custom Shared Program Folder* (Власна папка Програми). Визначає розташування папки, що містить ярлики, які з'являються в папці Programs (Програми) меню кнопки Start (Пуск).
- *Custom Desktop Icons/Custom Shared Desktop Icons* (Власні значки робочого столу). Визначає розташування папки, що містить ярлики, які з'являються на робочому столі Windows.
- *Custom Startup Folder/Custom Shared Startup Folder* (Власна папка Автозавантаження). Визначає розташування папки, що містить ярлики, які з'являються в папці Startup (Автозавантаження) меню кнопки Start (Пуск).
- *Custom Start menu/Custom Shared Start menu* (Власна папка Головне меню). Визначає розташування папки, що містить ярлики, які з'являються в меню кнопки Start (Пуск).
- *Hide Start menu Subfolders* (приховати папки, вкладені в папку Головне меню). Блокує появу в меню кнопки Start (Пуск) вкладених папок, які входять у профіль користувача, щоб запобігти дублювання з папками, визначеними в попередніх політиках.

Ці системні політики мають різні імена залежно від того, в яких ОС Windows вони застосовуються.

2.2.5.3 Захист файлової системи

Обмеження доступу до файлової системи – це ще один спосіб захисту робочих станцій. Якщо операційні системи і додатки на всіх робочих станціях мережі вже попередньо сконфігуровані, а користувачі сповіщені про необхідність зберігати всі робочі файли на дисках серверів, то не залишається жодної вагомої причини для того, щоб користувачам як і раніше було необхідно мати прямий доступ до локальної файлової системи. Блокування цього доступу за допомогою системної політики дозволить не допустити переміщення, зміни чи видалення файлів, необхідних для функціонування операційної системи робочої станції. Також можна обмежити і доступ користувачів у мережу, застосовуючи правила політики, перераховані нижче.

- *Hide Drives in My Computer* (приховати диски в папці Мій комп'ютер). Блокується поява всіх букв, що позначають диски у папці My Computer (Мій комп'ютер), включаючи і локальні, і мережеві диски.
- *Hide Network Neighborhood* (приховати мережеве оточення). Блокує появу піктограми Network Neighborhood (Мережеве оточення) на робочому столі Windows і забороняє з'єднання з застосуванням UNC-імен. Наприклад, якщо це правило політики дозволене, користувачі не можуть одержати доступ до мережевих дисків за допомогою відкриття вікна з UNC-ім'ям у діалоговому вікні Run (Виконати).
- *No Entire Network in Network Neighborhood* (приховати значок Уся мережа в мережевому оточенні). Блокує піктограму Entire Network (Уся мережа) у вікні Network Neighborhood (Мережеве оточення), не дозволяючи користувачам переглядати ресурси за межами домену чи робочої групи.
- *No Workgroup Contents in Network Neighborhood* (Не показувати склад робочих груп). Блокує піктограми, що є системами поточного домену чи робочої групи у вікні Network Neighborhood (Мережеве оточення).
- *Remove Find Command from Start menu* (Видалити команду Пошук). Видаляє команду Find (Пошук), не дозволяючи користувачам одержувати доступ до дисків, що можуть бути захищені від нього іншими способами. Якщо, наприклад, атрибут Hidden використовується для захисту локальної файлової системи, то команда Find (Пошук) як і раніше зможе вести пошук на локальному диску, а також дозволить бачити сховані файли.

Блокування файлової системи – це дуже радикальний крок, який потрібно ретельно зважити і спланувати. Лише деякі типи користувачів відчують переваги при такому обмежувальному підході, інші ж можуть дуже сильно на нього образитися.

Насамперед необхідно переконатися в тому, що системна політика, яка використовується для обмеження доступу до робочих станцій, не погіршує рівня функціональності, необхідного користувачам для виконання їхньої повсякденної роботи, а також у тому, що до можливостей, які планується обмежити, відмовлений доступ іншими способами. Наприклад, мо-

жна заборонити доступ до панелі керування, видаливши відповідну папку з групи Settings (Настроювання) у меню кнопки Start (Пуск), однак користувачі як і раніше зможуть одержувати до неї доступ за допомогою вікна My Computer (Мій комп'ютер) чи діалогового вікна Run (Виконати), якщо і ці варіанти також не будуть заблоковані.

2.2.6 Застосування системної політики

Саме по собі використання системної політики в системі Windows контролюється політикою за назвою Remote Update, яка застосовна до будь-якої операційної системи Windows. Ця політика має три можливі установлення:

- *Off* (Вимкнено). Система не використовує політику зовсім;
- *Automatic* (Автоматично). Система автоматично перевіряє кореневий каталог ресурсу спільного використання контролера домену, що проводив її аутентифікацію, на предмет присутності файлу політики;
- *Manual* (Ручне). Система проводить пошук файлу системної політики в каталозі, зазначеному як значення іншого правила політики за назвою Path for Manual Update (Шлях при відновленні в ручному режимі).

Використовуючи політику Remote Update, можна сконфігурувати системи для одержання файлів системної політики з місця їхнього розташування за замовчуванням, а також з будь-якої області, що буде зазначена. Для того, щоб робочі станції мали можливість доступу до файлів системної політики в будь-який час, здійснюється їх реплікація на всі контролери домену як в автоматичному, так і в ручному режимі, аналогічно профілям користувачів.

2.2.6.1 Віддалене редагування реєстру

Крім методів попередньої конфігурації, таких як профілі користувачів або системна політика, можлива також інтерактивна взаємодія з реєстром робочої станції Windows, навіть з віддаленого місця, за допомогою декількох різних інструментів.

Редактор реєстру Windows (regedit.exe) дає можливість встановлювати з'єднання з іншою системою мережі й одержання доступу до її реєстру. Крім того, можна використовувати редактор системної політики для інтерактивної модифікації реєстру локальної чи віддаленої системи. Однак доступ до реєстру, що забезпечує SPE, обмежується лише тими установленнями реєстру, які визначені в шаблонах системної політики, завантажених у даний момент.

2.2.6.2 Групові політики Windows

Операційна система Windows, що підтримує використання системної політики, надає таку можливість, як створення групових політик (group policies), що в поєднанні з Active Directory використовуються для ство-

рення комплексних конфігурацій робочих станцій. Крім можливостей політики Windows, які пов'язані зі зміною реєстру, групові політики можуть включати такі правила:

– Правила політики, що містить установлення системи безпеки локального комп'ютера, домену чи мережі;

– Правила політики установлення й обслуговування програмного за безпечення;

– Правила політики, що дозволяють адміністратору віддалено проводити інсталяцію, відновлення версій, виправлення і видалення програмного забезпечення робочої станції;

– Правила політики, що реалізують певні скрипти підключення до мережі і відключення від мережі для конкретних користувачів за допомогою всіляких мов написання скриптів, які підтримуються Windows Scripting Host;

– Правила політики, що переміщають певні каталоги користувачів на мережеві диски, де до них може одержати доступ будь-яка система.

Можна здійснювати реалізацію групових політик, створюючи об'єкти групової політики в консолях, що входять у Active Directory операційної системи Windows, наприклад, Active Directory Users and Computers. Створивши об'єкт групової політики, його можна асоціювати з будь-яким ін.-шим об'єктом Active Directory, щоб поширити на нього дію даної політики.

2.3 Керування робочим середовищем користувачів

В організації, що складається з досвідчених користувачів, кожен користувач може самостійно конфігурувати робочий стіл Windows. Користувачі можуть створювати свої піктограми на робочому столі, здійснювати керування власними ярликами меню кнопки Start (Пуск), самостійно вказувати букви для позначення дисків. Проте далеко не будь-яка організація може похвалитися великою кількістю досвідчених користувачів, і тому набагато доцільніше надати адміністратору мережі можливість сформувати стабільну і життєздатну конфігурацію робочих станцій.

2.3.1 Відображення дисків

Деякі користувачі не мають чіткого уявлення про сутність мережі і про те, як диск сервера може позначатися певною буквою на локальній машині. Користувач може мати диск, позначений буквою F, що відповідає диску певного сервера, і думати, що системи інших користувачів сконфігуровані у такий самий спосіб. Якщо розподіл букв для позначення дисків на робочих станціях не є постійним, можуть виникати непорозуміння, коли, наприклад, один користувач вказує іншому, що файл знаходиться на диску F, а фактично ця буква відповідає зовсім іншому диску спільного використання. Для того, щоб уникнути подібних складностей, адміністра-

торам варто створити стратегію стабільного відображення дисків для користувачів, які спільно застосовують загальні ресурси.

Якщо в мережі є сервери додатків, що надають свої ресурси всім користувачам мережі (наприклад, сервер бази даних компанії), тоді кожна система мережі повинна позначати диск цього сервера однією і тією самою літерою. Реалізація таких мінімальних заходів дозволить значно зменшити кількість звернень користувачів до служби технічної підтримки мережі.

Для реалізації стабільного набору букв, що відповідають дискам користувачів, можна застосовувати скрипти входу в мережу. Вони містять команди NET USE, що відображають диски серверів при кожному підключенні користувача до мережі. Правильне структурування цих команд дозволить створити єдиний скрипт входу в мережу для багатьох користувачів.

Щоб позначити командний файл як файл скрипта входу в мережу, необхідно ім'я цього файлу вказати на вкладці Profile (Профіль) діалогового вікна Properties (Властивості) об'єкта даного користувача в консолі Users and Computers, що входить до Active Directory.

2.3.2 Профілі користувачів

Створення профілів користувачів є методом збереження ярликів і установлень конфігурації робочого столу індивідуальних користувачів у каталогах, до яких можливе одержання доступу в процесі запуску їхніх систем. Окремі профілі для кожного користувача дозволяють кожному з них повертати свої власні конфігураційні установлення при реєстрації в системі. Якщо профілі користувачів зберігаються на робочій станції, то стає можливим їх спільна експлуатація декількома користувачами, причому без необхідності перезаписувати конфігураційні установлення один одного. Якщо ж профілі зберігаються на сервері мережі, користувачі зможуть одержувати до них доступ з будь-якої робочої станції. Це називається переміщуваним профілем (roaming profile). Крім того, можна змусити користувачів завантажувати певний профіль при кожному вході в систему і заборонити їм змінювати профіль. Це буде називатися обов'язковим профілем (mandatory profile).

Системний реєстр Windows 95 і 98 складається з двох файлів на локальному диску під назвами System.dat і User.dat. Файл User.dat відповідає ключу реєстру HKEY_CURRENT_USER, що містить усі конфігураційні установлення, що мають відношення до користувача, зареєстрованого в даний момент. В операційних системах Windows 2000/XP Professional, Windows Server 2003 та Windows Vista Ultimate відповідний файл називається Ntuser.dat. Цей файл, також названий кущем реєстру (registry hive), формує основу профілю користувача. При завантаженні файлу User.dat чи Ntuser.dat у процесі старту системи, установки, що містяться в ньому, під'єднуються до системного реєстру і стають активними в даній системі.

Кущ користувача містить такі типи установок конфігурації:

– всі обумовлені користувачем установлення Windows Explorer (Провідник Windows);
– постійні з'єднання мережевих дисків;
– з'єднання мережевих принтерів;
– всі обумовлені користувачем установлення Control Panel (Панель керування);
– всі установлення панелі задач;
– всі обумовлені користувачем установлення допоміжних програм Windows, наприклад, Calculator (Калькулятор), Notepad (Блокнот), Clock (Годинник);
– усі закладки, створені в системі довідкових файлів Windows.

Крім самого куща профіль користувача може також включати підкаталоги, що містять ярлики й інші елементи, які формують конфігурацію робочого столу даного користувача. Ці підкаталоги перераховані нижче.

- *Application Data*. Містить дані, специфічні для додатків, наприклад, індивідуальні файли словників.
- *Cookies*. Містить cookies, які використовуються Internet Explorer для збереження інформації про взаємодію системи з деякими сайтами Інтернету.
- *Desktop* (Робочий стіл). Містить ярлики до програм і файлів, що з'являються на робочому столі Windows.
- *Favorites* (Обране). Містить ярлики програм, файлів і URL, що з'являються в списку Favorites браузера Internet Explorer.
- *History*. Містить ярлики URL, які раніше були відвідані користувачем за допомогою Internet Explorer.
- *My Documents* (Мої документи). Містить ярлики особистих документів і інших файлів.
- *NetHood*. Містить ярлики, що з'являються у вікні Network Neighborhood (Мережеве оточення).
- *Personal*. Містить ярлики особистих документів і інших файлів.
- *PrintHood*. Містить ярлики, що з'являються у вікні Printers (Принтери).
- *Recent*. Містить ярлики, що з'являються в папці Documents (Документи) меню кнопки Start (Пуск).
- *SendTo*. Містить ярлики програм і областей файлової системи, що з'являються в папці SendTo (Відправити) контекстного меню.
- *Start menu* (Головне меню). Містить ярлики програм і файлів, що з'являються в меню кнопки Start (Пуск).
- *Templates* (Шаблони). Містить ярлики шаблонів документів.

Каталоги NetHood, PrintHood і Templates за замовчуванням є прихованими. Для того щоб переглянути їхній зміст Windows Explorer повинен бути сконфігурований для перегляду прихованих файлів.

За допомогою куща реєстру і підкаталогів профіль користувача конфігурує велику частину середовища робочої станції, включаючи такі елементи оформлення, як колір екрану і шпалер, робочі елементи, наприклад, піктограми робочого столу і ярлики меню кнопки Start (Пуск). Більш серйозні компоненти конфігурації системи, такі як драйвери чи пристрої їхньої установки, не входять у профіль користувача. Якщо у систему встановлюється нове обладнання, то всі користувачі будуть мати до нього доступ, незалежно від того, який профіль застосовується в даний момент.

За замовчуванням операційна система Windows створює окремий профіль для кожного користувача, що реєструється на даному ПК, і зберігає ці профілі в каталозі системного диска. Система також створює профіль користувача за замовчуванням у процесі власної інсталяції. Якщо є деякі елементи, які хотілося б включити в усі профілі даної системи, то можна внести відповідні зміни в цей профіль, що знаходиться в каталозі Default User, ще до того, як у системі зареєструється перший користувач. Після цього система буде копіювати профіль за замовчуванням у новий каталог при реєстрації кожного наступного користувача.

2.3.3 Створення переміщуваних профілів

ОС Windows зберігає профілі користувачів за замовчуванням на диску локальної машини. Можна змінити це установлення, вказавши місце для розташування конкретного профілю користувача на сервері мережі у вкладці Profile, де відзначається шлях до індивідуального каталогу даного користувача. Системи Windows працюють зі шляхом, зазначеним у полі Profile. Сервером профілів здатна стати будь-як система, до якої може бути отриманий доступ з робочої станції, причому вона може використовувати кожну з версій Windows і навіть Novell NetWare, SuSe Linux і т.д.

Як тільки зазначене місце розташування профілю, операційна система робочої станції робить копіювання активного профілю на диск сервера під час відключення користувача від мережі.

Найкращим способом організації системи профілів користувачів мережі є виділення одного ПК мережі як сервера профілів і створення на його диску каталогів з назвами, що відповідають іменам користувачів, у яких і будуть зберігатися профілі користувачів. Потім для задання розташування каталогу профілю кожного користувача можна використовувати змінну %username% як частину шляху, наприклад:

```
\\Ntserver\Profiles\%Username%
```

Після чого система самостійно замінить змінну %username% ім’ям користувача, під яким він пройшов реєстрацію. Однак ця змінна повинна зустрічатися в позначенні шляху лише один раз і відповідати тільки останньому підкаталогу. З іншого боку, система може розпізнавати розширення, які присвоюються цій змінній, що робить припустимими такі варіанти шляхів, як \\Ntserver\Profiles\%Username%.man.

Збереження профілів користувачів на сервері не приводить до їхнього видалення з тієї робочої станції, звідки вони здійснюються. Як тільки створено профіль, розміщений на сервері, кожна реєстрація користувача запускає такий процес: робоча станція порівнює профіль сервера з профілем, що знаходиться на самій робочій станції; якщо версія профілю сервера виявляється більш новою, ніж версія робочої станції, остання проводить його копіювання із сервера на локальний диск і вже звідти завантажує його в пам'ять; якщо обидва профілі ідентичні, робоча станція просто завантажує в пам'ять профіль, що є наявним на локальному диску, не переписуючи його із сервера. Коли користувач відключається від мережі, робоча станція вносить як у власну версію профілю, так і у версію робочої станції усі зміни, зроблені користувачем у ключах реєстру і ярликах робочого столу, які формують профіль.

Оскільки профіль завжди завантажується тільки з локального диска, навіть у тому випадку, коли його версія копіюється із сервера, важливо брати до уваги наслідки тих змін, які вносяться в профіль з іншого ПК. Якщо, наприклад, адміністратор змінює профіль на сервері, видаляючи деякі ярлики, то ці маніпуляції, швидше за все, ні до чого не приведуть, оскільки ярлики все одно збережуться на робочій станції, і копіювання профілю сервера не викликає їх видалення. Для зміни профілю необхідно внести відповідні корективи як у копію сервера, так і в копію робочої станції.

Як тільки створений профіль користувача розміщений на сервері, цей користувач може підключатися до мережі через будь-яку робочу станцію і завантажувати власний профіль, крім невеликого обмеження: профілі користувачів, створені різними ОС Windows, не є взаємозамінними, тому що реєстри цих операційних систем принципово різні: користувач, що має профіль Windows XP Professional, Windows Server 2003 чи Windows Vista Ultimate на сервері, не зможе входити в мережу з робочих станцій Windows 98 і завантажувати той самий профіль чи використовувати той самий каталог сервера для збереження ще і профілю Windows 98.

Один з потенційних недоліків збереження профілів серверів на сервері мережі полягає в тому, що певну кількість даних регулярно потрібно передавати по мережі. Кущ реєстру і всілякі підкаталоги з ярликами зазвичай не викликають складностей. Однак, якщо, наприклад, користувач Windows XP Professional зберігає багато мегабайтів даних у таких каталогах, як My Documents чи Personal, то і час, необхідний для копіювання цих каталогів на сервер і зчитування їх назад, може призводити до значних затримок у процесі підключення до мережі і відключення від неї. Причина включення таких каталогів, як My Documents чи Personal, полягає в необхідності забезпечити користувачу доступ до його персональних робочих файлів, навіть якщо він підключається до мережі з іншої робочої станції. Якщо ж усі робочі файли користувачів уже зберігаються на сервері, як було рекомен-

довано раніше, то це не є необхідним, тому варто проінструктувати користувачів, щоб вони не зберігали великі обсяги інформації у цих каталогах.

2.3.4 Створення обов'язкових профілів

Коли користувачі модифікують елементи своєї конфігурації Windows, робоча станція вносить ці зміни у відповідні профілі користувачів, щоб вони зберігали свою дію при наступних підключеннях цих користувачів до мережі. Однак є можливість створення адміністратором мережі обов'язкових профілів, які користувачам не дозволено змінювати. Таким чином, при кожному наступному підключенні до мережі конфігурація системи буде залишатися незмінною, незалежно від того, які модифікації були внесені користувачами в процесі останнього сеансу роботи. Для того, щоб не допустити зміни користувачами власних профілів, коли вони відключаються від мережі, варто змінити ім'я куща реєстру в каталозі сервера, де зберігається профіль, з User.dat на User.man чи з Ntuser.dat на Ntuser.man. Коли робоча станція виявляє файл із розширенням man у каталозі профілю, вона завантажує саме його, а не файл із розширенням dat, і не переписує нічого в каталог профілю в процесі відключення користувача від мережі.

Створюючи обов'язковий профіль, варто переконатися в тому, що відповідний користувач у даний момент не працює і не зареєстрований на робочій станції. В іншому випадку кущ буде переписаний назад у файл із розширенням dat під час виходу користувача із системи.

Інша зміна, яку можна зробити, щоб переконатися що саме обов'язковий профіль буде використовуватися, полягає в присвоєнні розширення man самому каталогу, де знаходиться профіль. Це не дозволить користувачу пройти реєстрацію в мережі, не завантаживши профіль. Якщо сервер, на якому зберігається профіль даного користувача, виявиться недоступним, користувач просто не зможе підключитися до мережі. Якщо прийнято рішення зробити саме так, то варто переконатися в тому, що розширення man не тільки є наявним у самого каталогу, але і в шляху, що вказує розташування каталогу профілю, у вкладці Profile діалогового вікна Properties об'єкта.

Важливо розуміти, що перетворення профілів в обов'язкові не забороняє користувачам вносити зміни в конфігурації їхніх робочих станцій, а просто не дозволяє зберігати ці зміни в самому профілі. Крім того, сам по собі обов'язковий профіль не перешкодить користувачу вручну змінити профіль за допомогою видалення чи додання ярликів одержання доступу до куща реєстру. Якщо хочеться забезпечити вищий рівень контролю над конфігурацією робочої станції і взагалі перешкодити внесенню користувачами яких-небудь змін в інтерфейс, то варто застосовувати інший механізм, наприклад, системну політику, а також переконатися у тому, що каталоги профілів на сервері надійно захищені правами файлової системи.

2.3.5 Реплікація профілів

Якщо в питаннях забезпечення конфігурації робочих станцій передбачається опиратися на розміщення профілів користувачів на сервері, то варто обов'язково встановити ряд заходів для того, щоб ці профілі завжди залишалися доступними користувачам, коли б вони не підключалися до мережі. Це особливо важливо в тому випадку, коли застосовуються обов'язкові профілі з розширенням man, оскільки якщо сервер, де зберігаються ці профілі, несправний чи недоступний, користувачі з такими профілями просто не зможуть зареєструватися в системі. Один зі способів реалізації цієї ідеї полягає в розміщенні каталогів профілів на контролері домену і наступному використанні сервісу Directory Replicator для регулярного копіювання цих каталогів на інші контролери домену в мережі.

Як тільки вдасться домогтися події, коли каталоги профілів будуть повторені на усіх контролерах домену, можна буде використовувати змінну %LogonServer% у шляху до профілю кожного користувача, щоб точно знати що вони завжди зможуть одержати доступ до своїх профілів, коли підключаються до мережі, наприклад:

\\ %LogonServer%\users\%UserName%

У процесі входу в мережу робоча станція замінить змінну %Logonserver% на ім'я того контролера домену, що проводив аутентифікацію користувача. Оскільки каталоги профілів повторені на усіх контролерах домену, робоча станція завжди буде мати доступ до профілів, поки доступний кожний з контролерів домену.

2.3.6 Створення мережевого профілю користувача за замовчуванням

Операційні системи Windows мають профіль користувача за замовчуванням, що застосовується як шаблон при створенні нових профілів. Як згадувалося раніше, його можна модифікувати, щоб усі профілі, створювані на даному ПК, мали ряд характеристик. Також є можливість створення профілю користувача за замовчуванням у мережі, щоб забезпечити однаковий набір сервісів будь-якого нового профілю, створюваного в мережі. За замовчуванням ресурс спільного використання Netlogon знаходиться в каталозі \Windows\PolicyDefinitions системного диска сервера.

2.3.7 Ініціатива нульового адміністрування Microsoft для Windows

Zero Administration Initiative (ZAI, Ініціатива нульового адміністрування) фірми Microsoft – це програма, що використовує такі інструменти, як профілі користувачів, системна політика й інші елементи, щоб побудувати певну конфігурацію робочої станції. Ця конфігурація повинна бути проста в установленні й експлуатації, а також забезпечувати користувачів набором можливостей, необхідних їм для роботи з повним чи практично повним включенням всіх можливостей.

Принцип ZAI випливає з філософії «мінімальних привілеїв». За замовчуванням робочі станції Windows залишаються «відкритими» після установлення ОС, а це означає, що користувач має повний контроль над всіма елементами як операційної, так і файлової систем. ZAI починає свою діяльність з «закритої» операційної системи, а потім надає користувачам доступ тільки до тих елементам, які їм дійсно необхідні. Це в більшості випадків означає повну відсутність доступу до інструментів для конфігурування системи, таких як Control Panel (Панель керування) чи редактори реєстру, а також обмеження користувача мінімальним набором ретельно підібраних додатків.

Основна мета ZAI полягає в автоматизації максимальної частки процесу установки робочої станції і зниженні загальної вартості її експлуатації. Останнє може бути досягнуте в зв'язку з тим, що обмеження взаємодії користувача з операційною системою здатне запобігти ушкодженню конфігурації робочої станції через установлення неліцензійного програмного забезпечення й ушкодження файлів операційної системи.

2.3.8 Компоненти ZAK

Zero Administration Kit (Набір засобів нульового адміністрування) фірми Microsoft (ZAK) був доступний і раніше у вигляді версій для Windows NT 4.0, Windows 95/98 і Windows NT Server Terminal Server Edition. ZAK включає два попередньо сформованих варіанти конфігурації робочих станцій, що є набором інструментів, які можна використовувати разом з можливостями операційної системи для реалізації варіантів конфігурації. Мета ZAK полягає не в тому, щоб забезпечити для мережі рішення, що вимагає нульового адміністрування, а в тому, щоб надати адміністратору мережі свого роду шаблон, на основі якого він зможе створювати власні варіанти конфігурації робочих станцій, що відповідають вимогам користувачів мережі.

Zero Administration Kit для Windows безкоштовно доступний на Web-сайті фірми Microsoft за адресою: http//www.microsoft.com/Windows/zak.

Два базових варіанти конфігурації, що входять до ZAK, носять назви TaskStation і AppStation. Конфігурація AppStation призначена для користувачів з мінімальними знаннями і досвідом в області обчислювальної техніки, що повинні розв'язувати мінімальну кількість задач. Серед таких користувачів можна назвати, наприклад, співробітників центру обробки замовлень, діяльність яких зводиться до базового прийняття замовлення або роботи з покупцями. Конфігурація TaskStation обмежена запуском єдиного додатка (у даному випадку браузера Internet Explorer), що цілком замінює оболонку програми Windows Explorer (Провідник Windows) операційної системи. Звичайний додаток функціонує в як інтерфейсна частина системи бази даних, яка забезпечує користувачів функціями й інформацією, необхідними для їхньої роботи.

Оскільки оболонка повністю замінюється додатком, комп'ютер не має піктограм робочого столу, панелі задач або меню кнопки Start (Пуск), і Internet Explorer автоматично завантажується під час запуску системи. Крім того, користувачі ізольовані від локальної файлової системи і мають доступ лише до мережевих дисків і тільки за допомогою єдиного додатка. Оскільки користувачі TaskStation позбавлені іншого інтерфейсу з операційною системою крім додатка, у них немає жодної можливості змінити параметри конфігурації системи, а захищена файлова система не дозволить їм модифікувати файли операційної системи і додатка на локальному жорсткому диску.

Конфігурація AppStation є менш обмеженою, ніж TaskStation і забезпечує велику гнучкість для користувачів. Система AppStation виконує ретельно підібраний набір додатків з диска сервера і зберігає оболонку Провідника, а також ряд стандартних елементів керування Windows, таких як панель задач і меню кнопки Start (Пуск). Однак зазначене меню обмежено тільки тими ярликами, які необхідні для запуску додатка. Користувачі, як і раніше, мають доступ до файлової системи, обмежений конкретними мережевими дисками і лише з застосуванням зазначених додатків. Користувачам недоступна панель керування чи будь-який інший елемент керування конфігуруванням системи, також вони позбавлені доступу до командного рядка через діалогове вікно Run (Виконати) чи сеансу MS-DOS.

Обмеження, що накладаються на робочу станцію в рамках конфігурацій AppStation і TaskStation, реалізуються в основному за допомогою застосування системних профілів і дозволів файлової системи. Крім того, ZAK включає програми, які можна застосовувати для блокування доступу до дисковода на робочих станціях, а також дозволяє проводити повне установлення робочої станції, включаючи операційну систему і додатки, з використанням процедури, заснованої на скриптах, яка не потребує втручання користувача чи адміністратора.

2.3.9 IntelliMirror

Операційна система Windows додає ще більше функціональності ZAK особливо своєю можливістю за назвою IntelliMirror. IntelliMirror являє собою сервіс, що зберігає повніший набір параметрів конфігурації робочих станцій на серверах мережі таким чином, що він може бути отриманий будь-якою системою в будь-який час. Цей принцип в основному подібний з переміщуваним профілем користувача, за винятком того, що крім стандартної інформації профілю IntelliMirror підтримує копії робочих файлів усіх користувачів і інформацію про додатки, установлені на кожній робочій станції. Кінцевий результат полягає в тому, що користувачі можуть підключатися до мережі з будь-якої робочої станції, причому система буде негайно завантажувати їхні власні додатки, робочі файли й установлення конфігурації, готові для застосування. У такий же спосіб, якщо в конкрет-

ної робочої станції відбувся збій апаратного забезпечення, адміністратори можуть дуже швидко і легко сконфігурувати новий комп'ютер для користувача без втрат даних користувача чи його особистих конфігураційних установлень.

Контрольні питання до розділу 2

1. Яким чином облікові записи впливають на систему безпеки операційної системи Windows NT?
2. Навести приклади та основні принципи шифрування.
3. Які типи довірчих відносин існують між доменами?
4. Яким чином можна переглянути облікові записи та їх властивості для різних груп.
5. Яка різниця між локальною та доменною політиками безпеки?
6. Визначити та охарактеризувати коло об'єктів, що стосуються конфігурування робочої станції.
7. Охарактеризувати вміст системного реєстру ОС MS Windows.
8. Обґрунтувати необхідність використання обов'язкових та переміщуваних профілів.
9. Вказати особливості збереження та доступу до профілю користувача.
10. Проаналізувати поняття системної політики та описати програмні засоби доступу до неї: редактор системної політики (SPE).
11. Особливості конфігурування персонального комп'ютера комп'ютерної мережі із урахуванням значень системної політики.
12. Обґрунтувати шляхи обмеження доступу користувачів у мережу.
13. Порівняти можливості ОС MS Windows різних версій.

Розділ 3
Файлові системи Windows NT

У Windows 2003 підтримуються три файлові системи:

– *NTFS* (New technology file system) – виключно для Windows NT;

– *FAT* (File Allocation Table) – для сумісності із застосуваннями MSDOS;

– *FAT 32* – модифікована версія FAT, використовувана в Windows 95 OSR2 і Windows 98.

Вибір файлової системи залежить від використовуваних застосувань і від вимог, які висуваються до неї. У кожної свої корисні властивості, але можливості захисту і аудиту систем різні.

Також в нових версіях Windows NT підтримуються розподілена файлова система DFS (Distributed File System) і файлова система з шифруванням EFS (Encrypted File System). Точніше, останні не є файловими системами у повній мірі, як, наприклад, FAT. DFS є розширенням мережевого сервісу і дозволяє об'єднувати у єдиний логічний том мережеві ресурси, розташовані на частинах з різними файловими системами. EFS – це надбудова над NTFS, що додає до останньої функції шифрування даних.

Проглядаючи ресурси комп'ютера, неможливо сказати, який формат має той або інший розділ жорсткого диска із такою ж впевненістю, як про гнучкі диски і CD/DVD-ROM. Розділи жорсткого диска позначені просто як *Local disk.* Щоб визначити тип файлової системи, треба натиснути праву кнопку миші на зображенні диска і в контекстному меню вибрати команду *Properties.* Додатково підтримується файлова система компакт-дисків CDFS.

3.1 Файлова система FAT

Файлова система FAT (File Allocation Table) одержала своє найменування відповідно до назви методу організації даних – таблиці розташування файлів. FAT спочатку була орієнтована на невеликі диски і прості структури каталогу. Через декілька років після створення її удосконалили для роботи з великими дисками і потужними персональними комп'ютерами. Організація диска із використанням файлової системи FAT має вигляд:

Блок параметрів BIOS	FAT1	FAT2 (копія)	Кореневий каталог	Область файлів

3.1.1 Дисковий розділ FAT

Кореневий каталог розташований на диску і має фіксоване місце. Каталоги – спеціальні файли з 32-бітовими елементами для кожного файлу, що міститься у цьому каталозі. Елемент для кожного файлу включає:

– ім'я файлу (8+3 символів);

– байт атрибуту (8 бітів);
– час модифікації (16 бітів);
– дату модифікації (16 бітів);
– місце розташування першого блоку (16 бітів);
– розмір файлу (32 біти).

Ця інформація використовується усіма операційними системами, що підтримують файлову систему FAT. Windows NT може зберігати і додаткові відмітки часу на елементі каталогу FAT. Ці елементи дозволяють визначити момент останнього доступу до файлу і використовуються в основному додатками POSIX.

Біти байта атрибуту файлу в елементі каталогу вказують, чи має файл відповідні атрибути. Встановлений перший біт ідентифікує файл як підкаталог; а другий – мітка тому. Зазвичай значеннями цих бітів керує операційна система. Крім того, файли FAT мають чотири спеціальні атрибути, які вказують на особливості роботи з цими файлами. Розрізняються файли: архівний, системний, прихований і для читання.

Windows NT, починаючи з версії 3.5, використовує біти атрибуту для підтримки довгих (до 255 символів) імен файлів в розділах FAT. Цей спосіб не заважає MS-DOS або OS/2 звертатися до подібного розділу. Коли користувач створює файл із довгим (що перевищує стандартне для FAT обмеження «8+3») ім’ям, Windows NT засновує елемент каталогу для цього файлу, відповідний угоді «8+3» (за тими правилами, що і для NTFS) із доданням одного або декількох вторинних елементів каталогу. Кожний з таких вторинних елементів розрахований на 13 символів у довгому імені файлу і зберігає довгу частину імені файлу в UNICODE. Для цих елементів встановлюються атрибути: том, системний, прихований, тільки для читання. MS-DOS і OS/2 ігнорують елементи каталогу з таким набором атрибутів, і останні невидимі в цих операційних системах. Замість них MS-DOS і OS/2 звертаються до елементів, що містять інформацію в стандартному вигляді «8+3».

Деякі дискові утиліти сторонніх виробників, взаємодіючи безносередньо з FAT, можуть розцінювати створені Windows NT елементи каталогу з довгим ім’ям файлу як помилки логічної структури тома. Спроби цих утиліт виправити помилки можуть призвести до втрати файлів і каталогів. Щоб уникнути подібних негараздів, не рекомендується використовувати в Windows NT утиліти роботи з диском або його дефрагментації, якщо таке ПЗ не перевірене на сумісність.

Файлова система FAT є системою з точним записуванням, тобто при необхідності зміни структури тому дається команда запису на диск. Недолік такої системи – повільне виконання послідовних операцій записування: адже перше записування на диск повинно бути завершене до початку другого і т.д.

Допускається перенесення або копіювання файлів з тому FAT на NTFS. Але при виконанні зворотної операції інформація про права і альтернативні потоки буде втрачена.

Слід відмітити, що файлова система FAT не забезпечує захисту даних і їх автоматичного відновлення. Тому FAT використовується лише у тому випадку, коли на комп'ютері як альтернативна система встановлена MS-DOS або Windows 98, а також для даних на гнучких дисках. Невеликий завантажувальний розділ, який відформатовано під FAT, потрібний, крім того, для RISC-систем. У решті випадків використання FAT не рекомендується.

3.1.2 Файлова система FAT32

FAT32 – модифікована версія FAT, що дозволяє створювати розділи об'ємом більше 2 Гб. Крім того, вона дає можливість використовувати кластери меншого розміру, і, відповідно, ефективніше витрачати дисковий простір. Вперше ця файлова система з'явилася в Windows 95 OSR2.

У таблиці 3.1 порівнюються розміри кластерів, що встановлюються за замовчуванням для FAT і FAT32.

Таблиця 3.1 – Порівняння розміров кластерів у FAT і FAT32

Об'єм диска	Розмір кластера на FAT	Розмір кластера на FAT32
0–32 Мбайтів	512 байтів	Не підтримується
32–б4 Мбайтів	1 Кбайтів	Не підтримується
64–127 Мбайтів	2 Кбайтів	Не підтримується
128–255 Мбайтів	4 Кбайтів	Не підтримується
256–511 Мбайтів	8 Кбайтів	Не підтримується
512–1023 Мбайтів	16 Кбайтів	4 Кбайтів
1024–2048 Мбайтів	32 Кбайтів	4 Кбайтів
260 Мбайтів – 8 Гбайтів	Не підтримується	4 Кбайтів
8–16 Гбайтів	Не підтримується	8 Кбайтів
16–32 Гбайтів	Не підтримується	16 Кбайтів
> 32 Гбайтів	Не підтримується	32 Кбайтів

3.2 Файлова система NTFS

Порівняно з FAT або FAT32, NTFS надає користувачу ціле поєднання переваг: ефективність, надійність і сумісність. Вона розроблена для швидкого виконання на дуже великих жорстких дисках операцій як стандартних файлових (типу читання, записування і пошуку), так і додаткових (наприлад, відновлення файлової системи).

Підтримуючи управління доступом до даних і привілеї власника, NTFS дає гарантії безпеки, потрібні для файлових серверів і персональних комп'ютерів в корпоративному середовищі. Це важливо для цілісності корпоративних даних.

NTFS проста, але дуже потужна розробка, для якої вся інформація на томі NTFS – файл або частина файлу. Кожен сектор на томі NTFS належить певному файлу. Частиною файлу є навіть метадані файлової системи (інформація, що описує безпосередньо файлову систему).

Ця заснована на атрибутах файлова система підтримує об’єктно-орієнтовані застосування, обробляючи всі файли як об'єкти з атрибутами, які визначено користувачем і системою.

3.2.1 Головна файлова таблиця

Кожен файл на томі NTFS поданий записом в спеціальному файлі – головній файловій таблиці MFT (Master File Table). NTFS резервує перші 16 записів таблиці для спеціальної інформації. Перший запис таблиці описує безпосередньо головну файлову таблицю. За нею йде дзеркальний запис MFT. Якщо перший запис MFT зруйнований, NTFS зчитує другий запис, щоб відшукати дзеркальний файл MFT, перший запис якого ідентичний першому запису MFT. Місцерозташування сегментів даних MFT і дзеркального файлу MFT записане в секторі початкового завантаження. Дублікат сектора початкового завантаження знаходиться в логічному центрі диска. Третій запис MFT – файл реєстрації – застосовується для відновлення файлів.

Сімнадцятий і подальші записи головної файлової таблиці використовуються власне файлами і каталогами на томі. На рисунку 3.1 показано спрощену структуру MFT, що забезпечує швидкий доступ до файлів.

3.2.2 Цілісність даних і відновлення в NTFS

NTFS – це відновлювана файлова система. У числі її переваг – поєднання швидкодії файлової системи з відкладеним записом і практично миттєве відновлення.

Кожна операція введення-виведення, яка змінює файл на томі NTFS, розглядається файловою системою як транзакція і може виконуватися як неподільний блок. При модифікації файлу користувачем сервіс файлу реєстрації фіксує всю інформацію, необхідну для повторення або відкату транзакції. Якщо транзакція завершена успішно, проводиться модифікація файлу. Якщо ні, то NTFS проводить повернення дії транзакції, виконуючи інструкції згідно з інформацією відміни. Якщо в транзакції виявлено помилку, транзакція виконується у зворотному порядку.

Файлова система відновлюється таким чином. При збої системи NTFS виконує три проходи: аналізу, повторів і відкатів. В процесі аналізу на підставі інформації файлу реєстрації NTFS оцінює пошкодження і точно визначає, які кластери потрібно модифікувати. Під час повторного проходу виконуються усі етапи транзакції від останньої контрольної точки. При поверненні відбувається відкат всіх незавершених транзакцій.

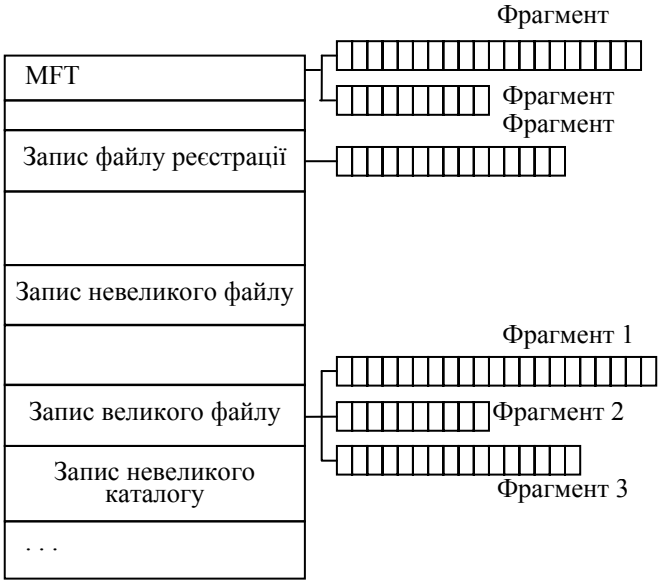

Рисунок 3.1 – Організація головної файлової таблиці

Об’єм журналу транзакцій встановлюється командою CHKDSK /L:розмір. Розмір вказується в кілобайтах і за замовчуванням дорівнює 4096 Кбайтів. Для того, щоб дізнатися поточний розмір журналу, не обхідно виконати команду CHKDSK /L.

3.2.3 Довгі і короткі імена файлів

Як вже наголошувалося, NTFS підтримує довгі (до 255 символів) імена файлів. У імені файлу використовуються символи UNICODE, що дозволяє іменувати файли, наприклад, кирилічними символами. При цьому вирішене питання доступу із MS-DOS: NTFS автоматично генерує стандартне для MS-DOS ім’я вигляду «8+3».

Якщо генерація коротких імен файлів не потрібна, то ця функція може бути відключена, для чого необхідно змінити значення параметра в реєстрі:

- гілка – HKEY_LOCAL_MACHINE;
- розділ – SYSTEM\CurrentControlSet\Control\FileSystem;
- параметр – NtfsDisable8dot3NameCreation;
- значення – 1;
- тип даних – DWORD.

Якщо значення цього параметра рівне 0 (за замовчуванням), то відбувається генерація коротких імен файлів, якщо 1 – генерація виконуватися не буде.

3.2.4 Компресія файлів і каталогів

Особливість NTFS – можливість динамічного ущільнення файлів і каталогів. Ущільнення є новим атрибутом файлу або каталогу і подібно до

будь-якого атрибуту може бути знято або встановлено у будь-який момент часу.

Ущільнення можливо тільки на розділах, розмір блоку яких не перевищує 4096 байт. Для установки розміру блоку використовується команда FORMAT /A:розмір.

Якщо каталог має атрибут Compressed, то всі файли, що копіюються в нього, також одержать цей атрибут. Якщо необхідно, щоб новостворюваний розділ диска автоматично ущільнював всі створювані і скопійовані на нього файли, його треба відформатувати з ключем /C, тобто:

FORMAT диск: /C /FS:NTFS.

Для ущільнення існуючого файлу або каталогу використовується або команда *Compress* або *Properties* у Windows NT Explorer.

За замовчуванням ущільнені файли не виділяються кольором при перегляданні тек. Для використання цієї можливості необхідно встановити відповідний прапорець у вікні *View Options*.

Ступінь ущільнення файлів залежить від типу файлу. Найефективніше застосовувати цей атрибут до файлів документів Microsoft Word, PowerPoint, графічних файлів і т.д. Організовуючи файл-сервер, має сенс ущільнити усі персональні каталоги користувачів. З іншого боку, абсолютно непродуктивно ущільнювати каталоги, що містять дистрибутиви програмних продуктів, які, як правило, уже ущільнені.

3.2.5 Створення і модифікація розділів диска

У ранніх версіях Windows NT для створення нових розділів на диску, їх форматування, призначення томам букв, дзеркалізації та інших режимів підвищеної надійності використовується програма Disk Administrator, яка має графічний інтерфейс.

Починаючи з Windows 2000 для управління системою використовується єдиний інструмент – MMC. Для конфігурування дисків необхідно відкрити призначений для цього зліпок (snap-in). Після його завантаження вікно консолі управління стане схожим на вікно програми адміністратора дисків, ранніх версій.

Команда FORMAT як і раніше присутня в системі, але містить ряд додаткових або модифікованих ключів:

```
FORMAT drive: [/FS:file-system] [/V:label] [/Q] [/A:size] [/C] [/E]
```

де:

– /FS : file-system – вказує тип файлової системи (FAT, FAT32, NTFS);
– /V: label – вказує мітку тому;
– /Q – виконує швидке форматування;
– /C – указує, що файли, які будуть записуватись на новий том, за замовчуванням, будуть ущільнюватись;
– /E – дозволяє оновлення тому (при цьому дозволяється використання усіх розширених функцій NTFS);

– /A:size – указує на використання блоків розміщення, розмір яких відрізняється від встановленого за замовчуванням.

Якщо клацнути правою кнопкою миші на назві диску в Windows NT Explorer, а потім вибрати в меню команду FORMAT, то запуститься графічна програма форматування дисків, яка зручніша для роботи, ніж її консольна реалізація.

3.2.6 Перетворення існуючого розділу у формат NTFS

Команда CONVERT дозволяє перетворити розділи FAT або FAT32 у розділ NTFS без втрати даних.

```
CONVERT диск: /FS:NTFS [/V]
```

де:

– диск – указує диск, на якому змінюється файлова система на NTFS (перетворення активного диска неможливе);
– /FS:NTFS – указує тип файлової системи (NTFS);
– /V – наказує програмі CONVERT виводити інформацію про роботу.

Єдине, про що необхідно пам’ятати при перетворенні, це про неможливість перетворення активного розділу – його доведеться відкласти до наступного перезавантаження операційної системи.

3.3 Розподілена файлова система

Розподілена файлова система DFS (Distributed File System) дозволяє об’єднати сервери і ресурси, що надаються в загальне користування, у простіший простір імен. DFS здійснює для серверів і ресурсів, які спільно використовуються на серверах, те саме, що файлові системи – для жорсткого диска. Файлові системи забезпечують однорідний поіменний доступ до набору секторів на дисках. DFS забезпечує однорідний поіменний доступ до набору серверів, ресурсів і файлів, які спільно використовуються, організовуючи їх у вигляді ієрархічної структури. У свою чергу, новий том DFS може бути ієрархічно підключений до інших ресурсів Windows NT, які спільно використовуються. Таким чином, DFS дозволяє організувати фізичні пристрої зберігання у логічні елементи, що у свою чергу, робить фізичне розташування даних прозорим як для користувачів, так і для застосувань.

3.3.1 Переваги DFS

Ієрархічний вигляд спільно використовуваних мережевих ресурсів, що настроюється. Пов'язуючи мережеві ресурси один з одним, адміністратори можуть створювати єдиний ієрархічний том у вигляді величезного жорсткого диска. Окремі користувачі можуть створювати свої власні томи DFS, які, у свою чергу, можуть бути включені в інші томи DFS. Це називається інтер-DFS зв’язок.

Гнучке адміністрування тому. Окремі мережеві ресурси, що входять до DFS, можуть бути відключені без будь-якого впливу на інші, що дозволяє адміністраторам управляти фізичними компонентами ресурсів без зміни їх логічного уявлення для користувачів.

Графічні засоби адміністрування. Кожен корінь DFS може управлятися за допомогою простого графічного інструмента, що дозволяє переглядати томи, змінювати їх конфігурацію, встановлювати інтер-DFS зв’язки, а також управляти віддаленим коренем DFS.

Підвищена доступність даних. Декілька мережевих ресурсів, наданих у спільне користування тільки для читання, можуть бути об'єднані під одним логічним ім'ям DFS. Якщо один з ресурсів недоступний, автоматично стає доступним альтернативний.

Балансування навантаження. Декілька мережевих ресурсів, наданих у спільне користування тільки для читання, і об'єднаних під одним логічним ім'ям DFS, дозволяють здійснювати балансування навантаження між дис.-ками або серверами. При доступі до такого ресурсу користувач автоматично переспрямовується на один з серверів, що входять в том DFS.

Прозорість імен. Користувачі пересуваються по простору імен незалежно від фізичного розташування даних. Дані можуть бути переміщені на будь-якому сервері, але подальша переконфігурація DFS робить це переміщення непомітним для користувача, оскільки він як і раніше оперує існуючим для нього простором імен DFS.

Інтеграція з моделлю безпеки Windows NT. Непотрібно ніяких додаткових заходів безпеки. Будь-який користувач, підключений до DFS, має доступ до ресурсів тільки в тому випадку, коли має відповідні права. При цьому використовується модель безпеки Windows NT.

Інтелектуальне кешування на клієнтській частині. Потенційно том DFS може об’єднувати сотні тисяч наданих у спільне використання ресурсів. На клієнтській стороні не робиться ніяких припущень про те, до якої частки інформації користувач може здійснювати доступ. Тому при першому зверненні до каталогу певна інформація кешується локально. При повторному зверненні до тієї ж інформації використовується частина, що знаходиться в кеші. Це дозволяє значно підвищити продуктивність у великих ієрархічних мережах.

Будь-який том, до якого можна здійснити доступ через редиректор Windows NT, може бути включений у простір імен DFS. Такий доступ здійснюється або за допомогою клієнтських редиректорів, або за допомогою шлюзів на сервері.

3.3.2 Технічний огляд розподіленої файлової системи

Корінь DFS – локальний ресурс, що надається в спільне користування і використовується як точка відліку для всієї решти ресурсів. Будь-який ресурс, що надається в спільне користування, може бути включений до про-

стору імен DFS. Доступ до тому DFS здійснюється за допомогою універсальної угоди про імена (UNC):

\Ім'я_сервера\Ім'я_ресурса_СВ\шлях\файл

де:

– ім'я_сервера – ім'я комп'ютера, який є хостом DFS;

– ім'я_ресурса_СВ – відповідає будь-якому ресурсу, який спільно використовується і який призначений коренем DFS;

– ім'я\шлях – будь-яке правільне ім'я файлу.

Хост тому DFS. У мережі допустимо безліч окремих томів DFS, кожен із своїм ім'ям. Будь-який сервер Windows NT (версії 4.0 і пізніше) може виконувати сервіс DFS і бути хостом тому DFS. Починаючи із версії Windows 2000 сервер може бути хостом для декількох томів DFS.

Зазвичай том DFS складається із покажчиків на безліч томів, що належать іншим серверам організації. Припустимо, наприклад, що в крупній проектній організації декілька груп користувачів працюють з текстовими документами. Необхідні їм документи розташовуються на різних серверах в самих різних ресурсах. За допомогою DFS можна об'єднати всі ці ресурси в один логічний том і тим самим значно полегшити працю згаданих співробітників. Приклад такого об'єднання для співробітника «Олена» показаний в таблиці 3.2.

Таблиця 3.2 – Об'єднання ресурсів системи до одного логічного тому

Ім'я UNC	Проектується на	Опис
\\Server\Public	\\Server\Public	Корінь DFS організації
\\Server\Public\Intranet	\\IIS\Root	Перехід на кореневий каталог інтрамережі
\\Server\Public\Intranet\ Corpinfo	\\Marketing\Info\ CorporateHTM	Перехід на каталог підрозділу в інтрамережі
\\Server\Public\Users	\\Server\Public\Users	Домашні каталоги користувачів
\\Server\Public\Users\Lena	\\Dev\NT\Priv\Users\ Lena	Перехід з Users в персональний каталог Олени на корпоративному сервері розробників
\\Server\Public\Users\ Lena \ ActiveX	\\ Lena1\Data\ActiveX	Перехід з персонального каталогу Олени на сервері в каталог на одній з його робочих станцій
\\Server\Public\Users\ Lena \ ActiveX	\\ Lena2\DataBackup\ActiveX	Альтернативний том: резервна копія робочих файлів Олени
\\Server\Public\Users\Sergey	\\NW51\Public\Users\Sergey	Том низького рівня: перехід на не-SMB том (такий як Netware або NFS)

Альтернативні томи. Якщо два або більше спільно використовуваних ресурсів є точною копією певного ресурсу, то їх можна помістити у про-

стір DFS під одним ім'ям. При цьому DFS не перевіряє реплікативність ресурсів. Організація реплікації покладається на адміністратора. Якщо реплікація не застосовується, то такі томи можна використовувати тільки для читання. У DFS можливі не більше 32 альтернатив у кожній точці переходу, а ось число точок переходу необмежене.

Томи низького рівня. Такими є всі томи, розташовані не на серверах Windows NT. Ці томи можуть бути створені в структурі DFS, але не можуть служити точками переходу або хостами DFS. До таких систем відносяться Windows NT Workstation, Windows XP Professional, а також всі мережеві ресурси інших виробників, до яких є доступ.

3.3.3 Робота з DFS

Адміністрування. Утиліта для адміністрування DFS дозволяє спростити управління, а також зміну конфігурації сервера. При першому запуску цієї утиліти буде запропоновано вибрати наявний корінь або створити новий (коренем може служити будь-який спільно використовуваний мережевий ресурс сервера). Після цього, використовуючи команди меню, можна створювати як нові елементи томів, так і альтернативні томи.

Робота кінцевих користувачів. Якщо на клієнтській стороні встановлена підтримка DFS, то доступ до будь-якого ресурсу DFS здійснюється точно так, як і до будь-якого звичайного мережевого ресурсу. Якщо використовується Explorer Windows NT або Windows 9x, то логічне дерево DFS в ньому відображається у вигляді дерева каталогів.

Внаслідок того, що простір імен DFS є логічним, адміністратор може призначати ресурсам змістовні імена, що також полегшує пошук потрібної інформації. Обмеження довжини стандартне для 32-розрядних версій Windows: довжина шляху не може перевищувати 260 символів.

Вже наголошувалося, що можливість створення альтернатив підвищує доступність даних і дозволяє балансувати навантаження серверів. Оскільки дана функція абсолютно прозора для користувача, то нічого окрім додаткових переваг вона йому не дасть. Наприклад, при одночасному доступі великої групи користувачів до якогось ресурсу, розташованого на декількох альтернативних серверах, члени групи будуть автоматично розподілені між цими серверами приблизно порівну, що зменшить навантаження на кожний з серверів і підвищить продуктивність.

Альтернативні ресурси дозволяють зробити оновлення інформації абсолютно непомітним для користувача. Адміністратор може розміщувати нові дані не на тому сервері, до якого зараз звертаються клієнти, а на іншому, який тимчасово недоступний для них. Після завершення оновлення і перевірки правильності досить перевизначити відповідне посилання у корені DFS, щоб користувачі отримали доступ до оновлених даних. При цьому клієнтам не потрібно нічого переналаштовувати.

Особливо це актуально для користувачів Інтернету або інтрамереж. Кожен підрозділ в організації може мати на своєму сервері окремий ресурс, що містить інформацію в HTML-форматі. Адміністратор, об'єднуючи такі розрізнені ресурси в дерево DFS, надає користувачам інтрамережі підприємства доступ до єдиного простору імен.

3.4 Файлова система із шифруванням

Один із стандартних запобіжних засобів в персональних комп'ютерах – можливість завантаження з гнучкого диска. Вона часто виручає при збоях на жорсткому диску або пошкодженні завантажувального сектора, оскільки дозволяє здійснити доступ до даних. На жаль, ця ж можливість дозволяє завантажити на комп'ютер операційну систему, відмінну від тієї, яка на ньому встановлена. Потенційно будь-яка особа, що має фізичний доступ до комп'ютера, зможе обійти систему обмеження доступу файлової системи Windows NT, використовуючи утиліти читання NTFS. Таким чином проблема захисту від несанкціонованого доступу залишається актуальною.

3.4.1 Архітектура EFS

Перш ніж говорити про використання файлової системи з шифруванням, необхідно ознайомитися з теоретичними основами: реалізацією процесів шифрування, дешифрування і відновлення файлів.

Криптографія. У EFS шифрування та дешифрування даних засновані на схемі із загальними ключами (public keys). Дані у файлі шифруються за допомогою швидкого симетричного алгоритму з використанням ключа шифрування файлів FEK (File encryption key). FEK – ключ певної довжини, що встановлюється або алгоритмом шифрування, або законом, що випадково генерується (в тому випадку, коли алгоритмом підтримуються ключі різної довжини).

Список зашифрованих FEK створюється з використанням загального ключа шифрування ключів одного або декількох користувачів. Для шифрування FEK використовується відкрита частина пари ключів користувача. Список зашифрованих FEK зберігається разом із зашифрованим файлом в спеціальному атрибуті EFS, полі дешифрації даних DDF (Data Decription Field). Інформація про шифрування файлу тісно пов'язана із самим файлом. Закрита частина пари ключів користувача служить для дешифрації і зберігається у надійному місці, наприклад в смарт-картах (smart cards) або інших захищених пристроях зберігання.

FEK також шифрується із використанням одного або декількох відкритих ключів відновлення ключів (recovery key keys). Для цього застосовується відкрита частина пари ключів, аналогічно уже описаному механізму. Список зашифрованих FEK зберігається разом із файлом в спеціальному атрибуті EFS, полі відновлення даних DRF (Data Recovery Field). Для шифрування

FEK, що зберігаються в DRF, потрібні тільки відкриті частини пар ключів відновлення. Для нормальної роботи файлової системи EFS відкриті ключі відновлення повинні бути постійно доступні. Операція відновлення – явище досить рідкісне і потреба в ній виникає тільки у разі звільнення спів робітника, втрати ключа і т.д. Отже, агенти відновлення (recovery agent) можуть зберігати закриті частини ключів у безпечному місці (інтелектуальні карти).

Звичайний текст, введений користувачем, шифрується за допомогою ключа FEK, який випадково згенерований. Цей ключ зберігається разом із файлом у двох полях: у полі дешифрації даних він зберігається зашифрованим відкритим ключем користувача, а у полі відновлення даних – відкритим ключем агента відновлення.

При дешифруванні закритим ключем користувача дешифрується ключ шифрування файлу FEK з відповідного поля дешифрування даних. FEK дешифрує дані, які прочитано, поблочно. При довільному доступі до великого файлу дешифруються тільки окремі блоки, а не весь файл.

Така проста схема забезпечує надійність технології шифрування і використання одного файлу декількома користувачами, а також можливість задіювати декілька агентів відновлення. В той же час, ця схема абсолютно «не прив'язана» до якого-небудь алгоритму і дозволяє застосовувати будь-який і, що дуже важливо, більш довершений алгоритм, який може з'явиться у майбутньому.

3.4.2 Робота з EFS

Робота в графічному інтерфейсі. Для доступу до функцій EFS із Explorer треба виділити файл(и) або каталог і натиснути на них правою кнопкою миші, а потім вибрати у контекстному меню команду *Encrypt.* Користувачу доступні дві команди *Encrypt (Зашифрувати)* і *Decrypt (Дешифрувати)*.

Шифрування. Ця операція дозволяє зашифрувати виділений файл. Якщо виділений каталог, то користувачу надається можливість вибрати, чи треба разом з каталогом шифрувати усі файли і підкаталоги в ньому.

Дешифрування. Ця операція зворотна шифруванню і дозволяє дешифрувати виділений файл. Додатково до дешифрування каталогу можна дешифрувати файли, які знаходяться у ньому.

Конфігурація. Користувачі мають можливість оперувати відкритими ключами, які використовують для шифрування файлів EFS: створювати, експортувати, імпортувати, а також управляти ними. Ця функція – для досвідчених користувачів, які хочуть управляти своїми ключами.

Шифрування файлів. Все, що потрібно, щоб зашифрувати файл, – виділити його і вибрати в контекстному меню команду *Encrypt*. З цієї миті файл зберігатиметься на диску в зашифрованому вигляді. Під час звернення до файлу для записування або читання у прозорий спосіб буде виконуватися шифрування або дешифрування. Щоб визначити, чи зашифрований

файл, користувачу досить подивитися, яка команда пропонується в контекстному меню (якщо *Encrypt*, то файл не зашифрований).

Оскільки шифрування прозоре, з погляду користувача, то він може продовжувати працювати з файлом точно так, як це робив і раніше: наприклад, використовувати для роботи з документом Microsoft Word, а для роботи із звичайним текстовим файлом – Notepad. При спробі доступу до цього файлу іншого користувача буде видане повідомлення про помилку доступу, оскільки відсутній відповідний ключ.

Адміністратори не повинні шифрувати файли системного каталогу. Це пов'язано з тим, що ці файли потрібні у момент завантаження системи, коли ключі шифрування ще недоступні. Для запобігання таким спробам Windows NT Explorer перешкоджає шифруванню файлів з атрибутом System. У майбутніх версіях Windows NT буде додана можливість захищеного завантаження, що дозволяє шифрувати системні файли.

У EFS є можливість імпорту (експорту) зашифрованих файлів між системами. Ці функції додані в команду *copy* і доступні із командного рядка.

Для експорту користувач повинен вказати зашифрований файл як початковий, а файл, який розташовано у незашифрованому каталозі – як приймальний. Експортований файл буде як і раніше зашифрований. Його можна копіювати на будь-яку іншу файлову систему, включаючи FAT, а також на магнітні стрічки пристроїв резервного копіювання; або «прикріпити» до електронного листа, подібно до звичайного файлу.

Щоб файл був доступний для використання на приймальній стороні, його необхідно імпортувати. Для цього користувач вказує як приймальний файл той, який розташовано на розділі NTFS.

При звичайному копіюванні зашифрованого файлу в каталог, який помічений як нешифрований, файл буде розшифрований і збережений у відкритому вигляді. Це пов'язано з тим, що операції шифрування і дешифрування прозорі для копіювання. Таку властивість можна використовувати при копіюванні файлів для широкого розповсюдження.

Шифрування каталогів. Позначити каталог як шифрований можна за допомогою команди *Encrypt* контекстного меню Windows NT Explorer. При цьому за замовчуванням всі файли в такому каталозі будуть зашифровані, а всі підкаталоги – помічені також як шифровані. Список файлів в каталозі не шифрується, тому за наявності відповідних прав доступу, його можна переглянути, як і раніше.

Позначаючи каталог як шифрований користувач може вказати, відноситься ця команда тільки до вибраного каталогу чи до усіх вкладених файлів і підкаталогів. Такий порядок полегшує користувачам турботу про захист своїх документів. Досить просто скопіювати файл в шифрований каталог або створити там новий файл, який буде негайно зашифрований.

Дешифрування файлів і каталогів. Зазвичай користувачам не потрібно дешифрувати файли або каталоги – адже, як вже наголошувалося, ця опе-

рація прозора як для користувача, так і для додатків. Проте якщо користувач хоче надати файл або каталог у спільне використання декільком колегам, то доведеться виконати дешифрування.

Дешифрування виконується аналогічно шифруванню – командою контекстного меню Windows NT Explorer. При застосуванні команди *Decrypt* до каталогу, користувач може вказати, чи відноситься вона до вкладених підкаталогів.

3.5 Квотування дискового простору

Починаючи із Windows 2000 з'явилася можливість квотування (обмеження) дискового простору, який надається користувачам.

Квотування виконується для кожного користувача і кожного дискового тому. Припустимо, що користувачі мають доступ до ресурсу \\Server\Public. Для користувачів цього ресурсу встановлено обмеження в 50 Мбайтів. Якщо користувач вичерпає свій ліміт в персональному каталозі \\Server\Public\Sergey і спробує створити (або скопіювати) файл в персональний каталог іншого користувача, то система завадить цьому.

До використаного дискового простору зараховують тільки файли, якими користувач володіє.

Реакція на перевищення користувачем встановленої квоти залежить від конфігурації системи. У будь-якому випадку в системний журнал буде внесений відповідний запис. Записи ведуться у хронологічному порядку, проте за замовчуванням в журналі не фіксується, які користувачі зараз перевищили межу. Якщо адміністратор задав відповідний параметр, то будь-яка спроба користувача записати що-небудь після перевищення ліміту закінчиться повідомленням про відмову в доступі внаслідок відсутності вільного простору.

Квотування диска дозволяється, якщо:

- розділ відформатовано під NTFS версії 5.0;
- є відповідні адміністративні повноваження.

Для виклику програми квотування треба натиснути правою кнопкою миші зображення диска і в контекстному меню вибрати команду *Properties.* Потім слід вибрати в діалоговому вікні *Disk Properties* вкладку *Quota.* Коли формат диска не NTFS, така вкладка не буде відображатись. Якщо формат диска NTFS 4.0 або немає адміністративних повноважень, на екрані з'явиться відповідне повідомлення.

Для активації функції квотування використовується прапорець *Enable quota management*. Якщо адміністратор бажає впливати на користувачів не тільки морально, слід встановити прапорець *Deny disk space to users exceeding quota limit* – тоді користувачам буде відмовлено у доступі при перевищенні виділеної квоти.

При перевищенні користувачем встановленого порогу попередження *(Set warning level to)* відбувається запис попередження в журнал.

Як уже згадувалося, із системного журналу не можна дізнатися, скільки користувачів перевищили встановлені для них пороги або наблизилися до порогу. Це можна з'ясувати, якщо в діалоговому вікні *Disk Properties* клацнути кнопку *Quota Entries*. Усі облікові записи, для яких перевищений поріг попередження, будуть відмічені відповідним значком.

Для модифікації встановлених квот треба двічі клацнути на відповідній квоті, а для додання нових обмежень – вибрати в меню *Quota* команду *Add New Quota*. З'явиться діалогове вікно *Quota Settings*. У цьому вікні указується ім'я облікового запису, для якого вводиться квотування, а також пороги попередження і використання.

3.5.1 Права на доступ до файлів і каталогів. Поняття власника

Права на доступ до файлів і каталогів визначають, чи може користувач здійснювати до них доступ і, якщо може, – то як саме. Користувач, який створив файл або каталог, є його власником. Володіння файлом або каталогом дозволяє користувачу змінювати права на доступ до нього. Адміністратор може вступити у володіння файлом або каталогом без згоди власника, але не може передати його назад у володіння колишньому власнику. Щоб передати володіння файлом, адміністратор повинен реєструватися під ім'ям іншого користувача і узяти файл у володіння.

Права на доступ до файлів і каталогів кумулятивні. Виняток становить No Access (немає доступу), що має перевагу над іншими. Припустимо, користувач Сергій має доступ до файлу FILE1 тільки на читання. Одночасно він входить до групи «Викладачі», що володіє правом *зміни (change)* файлу FILE1. Таким чином, Сергій має можливість як читання, так і змінення файлу FILE1. А ось якби Сергій входив до групи «Студенти», для якої встановлена заборона доступу до файлу, він теж не мав би доступу до цього файлу. Як випливає із наведеного прикладу, права кумулятивні, що не завжди зручно. Припустимо, що Сергій, який входить до групи «Викладачі», не повинен володіти можливістю змінювати файл FILE1. Тільки призначивши конкретну заборону можна позбавити його такої можливості, залишивши, в той же час, права *зміни (change)* для усіх інших користувачів групи «Викладачі».

Надання прав на доступ до файлів і каталогів – основа захисту в Windows NT. Доступ до всіх діалогових вікон, які управляють правами доступу, може здійснюватися безпосередньо із вікон, які відповідають текам, або із Windows NT Explorer. Для цього необхідно натиснути правою кнопкою миші ім'я потрібного файлу або теки і в контекстному меню вибрати *Properties*, а потім у діалоговому вікні *File Properties*, що з'являється, – вкладку *Security*.

3.5.2 Надання і заборона доступу до файлів

Щоб визначити доступ до файлу на розділі NTFS, необхідно вибрати у діалоговому вікні *File Properties* вкладку *Security*. На екрані з'явиться логове вікно із елементами *Name*, *Permissions*, *Allow*, *Deny* і *Inherit permis-*

sions from parent. Також доступний ряд кнопок для додання або виключення користувачів із списку доступу і модифікації доступу.

У списку *Name* знаходяться імена локальних груп і користувачів, для яких вказані права доступу до вибраного файлу. Імена користувачів показуються у форматі Ім'я_Домену\Ім'я_користувача. Для додання нових користувачів або груп треба натиснути кнопку *Add* і вибрати у списку, що з'явився, необхідне.

У розділі *Permissions* можна вибрати найзагальніші типи доступу до файлів і пов'язані із ними дії над файлами (таблиця 3.3). Окремо указуються як дозволи *(Allow)*, так і заборони *(Deny)*. За замовчуванням тип доступу до файлу успадковується від каталогу, в якому розташовується файл. Якщо спадкоємство із яких-небудь причин не підходить, слід прибрати прапорець *Inherit permissions from parent*.

Таблиця 3.3 – Типи доступу і операції над файлами

Дія	Full Control	Change	Read & Execute	Read	Write
Показувати дані файлу	+	+	+	+	
Показувати атрибути файлу	+	+	+	+	
Виконувати файл	+	+	+		
Показувати власника файлу та типи доступу	+	+	+	+	
Змінювати атрибути файлу	+	+			+
Змінювати та додавати дані	+	+			+
Видаляти файл	+	+			
Змінювати власника файлу та права доступу	+				

Якщо потрібна детальніше налаштування доступу до файлу, то слід натиснути кнопку *Advanced*. З'явиться діалогове вікно *Access Control Settings* із списком контролю доступу (ACL) вибраного файлу. Кожен рядок списку містить тип доступу (*Allow/Deny),* ім'я користувача, для якого визначено цей дозвіл, і назву дозволу. Крім вже згадуваних вище найзагальніших дозволів (*Full Control*, *Modify*, *Read & Execute*, *Read*, *Write*) можна встановити і спеціальний доступ (*Special*). Для редагування рядка слід або двічі клацнути на ньому, або скористатися кнопкою *View/Edit.*

3.5.3 Надання прав на доступ до каталогів

Для зміни дозволів доступу треба виділити каталог (або декілька каталогів), натиснути праву кнопку миші і у контекстному меню, що з'явилося, вибрати команду *Properties*, а потім вибрати у діалоговому вікні, що з'явилося, *Directory Properties* вкладку *Security*. Це діалогове вікно схоже із вікном *File Properties*, описаним раніше і призначеним для файлів. Відмінність – у списку дозволів, призначених (або заборонених) для каталогу. Як і для файлів тут наведений список тільки найзагальніших видів доступу.

Таблиця 3.4 – Типи доступу і операції над каталогами

Дія	Write	Read	List folder contents	Read & Execute	Change	Full Control
Показувати імена каталогів		+	+	+	+	+
Показувати атрибути каталогів		+	+	+	+	+
Переходити в підкаталоги			+	+	+	+
Змінювати атрибути каталогу	+				+	+
Створювати підкаталоги та додавати файли	+				+	+
Показувати власника каталогу та права доступу		+	+	+	+	+
Видаляти каталог					+	+
Видаляти будь-який файл або підкаталог						+
Змінювати власника каталогу						+
Змінювати права доступу до каталогу						+

Таблиця 3.5 – Права доступу до каталогів та дії над файлами

Дія	Write	Read	List folder contents	Read & Execute	Change	Full Control
Показувати дані файлу		+		+	+	+
Показувати атрибути файлу		+		+	+	+
Виконувати файл				+	+	+
Показувати власника файлу та типи доступу		+		+	+	+
Змінювати атрибути файлу	+				+	+
Змінювати та додавати дані	+				+	+
Видаляти файл					+	+
Змінювати власника файлу та права доступу						+

Для встановлення прав доступу, відмінних від загальних, можна скористатися редактором ACL так само, як і у випадку із файлами. Для виклику редактора треба використати кнопку *Advanced* – з'явиться діалогове вікно *Access Control Settings* із списком рядків ACL. Кожен рядок містить такі поля: *Allow/Deny* (тип доступу), ім'я користувача, дозвіл, а також застосовуваність. Під застосовуваністю розуміється глибина дії вказаного рядка ACL. Дозвіл може відноситися:

- тільки до цього каталогу;
- до цього каталогу і всіх вкладених підкаталогів і файлів;
- тільки до каталогу і підкаталогів;
- тільки до каталогу і файлів в ньому;
- тільки до підкаталогів і файлів;

– тільки до підкаталогів;
– тільки до файлів.

Для редагування рядків ACL треба скористатися кнопкою *View/Edit*. Після цього на екрані з'явиться діалогове вікно *Permission Entry*.

У ньому можна вказати ім'я облікового запису, для якого використовуватиметься даний рядок ACL, глибину дії і, звичайно ж, дозвіл (або заборона). Слід звернути увагу на прапорець *Apply these permissions down the tree*. Якщо він відмічений, то вказані дозволи будуть застосовані не тільки до об'єктів у списку *Apply onto*, але і до всіх наступних нижче по дереву об'єктів, для яких це можливо.

3.5.4 Володіння каталогами і файлами

За замовчуванням користувач, який створив каталог або файл, є його власником. У ранніх версіях Windows NT неможливо передати файл у володіння будь-кому іншому. Можна було тільки вступити у володіння – такою привілеєю за замовчуванням володіли адміністратори системи.

Починаючи з Windows 2000 поняття володіння дещо змінене. Тепер користувач (за наявності на те прав) може не тільки вступити у володіння файлом або каталогом, але і передати його у володіння третій особі. Цією особою може бути тільки користувач, який володіє відповідними повноваженнями, наприклад, адміністратор. Для визначення поточного власника файлу і (або) передачі володіння треба викликати діалогове вікно *Folder Properties*, вибрати вкладку *Security* і натиснути кнопку *Advanced*. У вікні редактора списку контролю доступу, що з'являється, треба вибрати вкладку *Owner*. У полі *Current owner of this item* буде показаний поточний власник об'єкта, а в списку *Change owner to* – облікові записи, що мають право вступити у володіння. Для того, щоб вступити у володіння, треба вибрати свій обліковий запис у списку (звичайно, якщо він там присутній) і натиснути *OK*.

Контрольні питання до розділу 3

1. Основні файлові системи ОС Windows. Їх переваги та недоліки.
2. Порівняти основні файлові системи з точки зору захищеності роботи з файлами.
3. Навести приклад організації файлової таблиці.
4. Склад розподіленої файлової системи.
5. Навести приклади роботи з основними файловими системами.
6. Навести основні особливості роботи з файловою системою із шифруванням.
7. Основні причини квотування дискового простору.
8. Які основні права на доступ до файлів і каталогів? Можливості їх зміни.

Розділ 4
Програмні засоби діагностування комп'ютерної мережі

Незважаючи на те, наскільки добре розроблена і встановлена мережа, виникають ситуації, коли вона перестає правильно працювати. Частина роботи адміністратора мережі полягає в щоденному контролі продуктивності мережі й усуненні будь-яких проблем, що можуть виникнути. Для цього необхідно мати відповідні засоби й інструменти. Порушення можуть виникнути фактично на будь-якому рівні, і засоби, які використовуються для діагностики проблем на різних рівнях, відповідно різняться. Знання доступних засобів є істотним моментом у боротьбі з несправностями.

4.1 Утиліти операційної системи Windows

Операційні системи Windows включають різні засоби, які можна застосовувати для керування мережевими з'єднаннями і виявлення пов'язаних з ними проблем. Більшість з цих програмних інструментів включені в усі ОС Windows, хоча вони можуть приймати різні форми.

4.1.1 NET

Команда NET є основним засобом управління з командного рядка для мережевого клієнта Windows. Цю команду можна використовувати для виконання багатьох мережевих функцій, схожих з тими, що дозволяють здійснювати графічні утиліти, такі як Windows Explorer (провідник Windows). Оскільки NET – утиліта командного рядка, то існує можливість включати її в скрипти реєстрації і командні файли. Наприклад, NET можна використовувати для входу і виходу з мережі, підключення мережевих ресурсів спільного використання, запуску і зупинення сервісів, розміщення в мережі спільних ресурсів.

Команда NET реалізована як файл з ім'ям Net.exe, що розміщується у системному каталозі у процесі інсталяції операційної системи. Щоб використовувати цю програму, треба запустити файл із командного рядка, указавши підкоманду, що може мати додаткові параметри. Хоча деякі підкоманди у різних версіях ОС Windows однакові, проте існують підкоманди унікальні для кожної з операційних систем. Ці підкоманди і їхнє призначення перераховані в табл. 4.1, а функції деяких ключів розглядаються в наступних розділах.

4.1.2 NET CONFIG

Команда NET CONFIG виводить на екран інформацію про мережевого клієнта, установленого на даній системі, таку як показана нижче:

```
Computer name                    WCZ5
User name                        CRAIGZ
```

```
Workgroup                              NTDOMAIN
Workstation root directory             C:\WINDOWS
Software version                       4.00.950
Redirector version                     4.00
The command was completed successfully.
```

Таблиця 4.1 – Варіанти команди NET операційних систем Windows

Підкоманда NET	**Призначення**
NET ACCOUNTS	Конфігурує установки і правила політики для всіх облікових записів деякого комп'ютера або домену
NET COMPUTER	Додає та видаляє комп'ютер з поточного домену
NET CONFIG	Виводить на екран інформацію про мережевого клієнта
NET CONFIG SERVER	Конфігурує параметри сервісу Server
NET CONFIG WORKSTATION	Конфігурує параметри сервісу Workstation
NET CONTINUE	Продовжує роботу сервісу, що був зупинений
NET DIAG	Обмін діагностичними повідомленнями з іншою системою, щоб перевірити з'єднання
NET FILE	Виводить на екран і закриває файли, які спільно використовуються користувачами мережі, а також знімає блокування файлів
NET GROUP	Створює та видаляє глобальні групи, а також додає/видаляє у цих групах користувачів
NET HELP	Виводить на екран довідку для визначених підкоманд NET
NET HELPMSG	Виводить на екран додаткову інформацію про чотиризначні коди помилки
NET INIT	Завантажує драйвери протоколів і мережевого адаптера без прив'язки їх до Менеджера протоколів (Protocol Manager)
NET LOCALGROUP	Створює/видаляє локальні групи, а також додає/видаляє у цих групах користувачів
NET LOGOFF	Здійснює вихід користувача з мережі і закриває з'єднання з усіма мережевими ресурсами спільного використання
NET LOGON	Проводить реєстрацію користувача у робочій групі чи групі домену
NET NAME	Керує списком імен, які використовуються сервісом Messenger для відправлення повідомлень
NET PASSWORD	Змінює пароль реєстрації у мережі поточного користувача
NET PAUSE	Припиняє роботу зазначеного сервісу без вивантаження його з пам'яті до того, як його робота буде відновлена командою NET CONTINUE
NET PRINT	Керує роботою черги друку і завданнями друку, які розміщені в ній
NET SEND	Передає текстове повідомлення іншому користувачу чи комп'ютеру, використовуючи сервіс Messenger
NET SESSION	Виводить на екран інформацію про поточні активні сесії з іншими користувачами мережі

Продовження таблиці 4.1

Підкоманда NET	Призначення
NET SHARE	Виводить на екран, створює та видаляє ресурси, надані в спільне використання на даному комп'ютері
NET START	Запускає вказаний мережевий сервіс
NET STATISTICS	Виводить на екран статистику для сервісів Server и Workstation
NET STOP	Зупиняє вказаний мережевий сервіс
NET TIME	Виводить на екран час, встановлений у даній системі, або синхронізує час з іншою системою
NET USE	Виводить на екран інформацію про з'єднання з мережевими ресурсами спільного використання і дозволяє керувати цими з'єднаннями
NET USER	Створює, змінює і видаляє облікові записи користувачів
NET VER	Виводить на екран тип і номер версії засобу переадресації робочої групи, який використовується в даний момент
NET VIEW	Виводить на екран ресурси, які доступні у мережі

4.1.3 NET DIAG

Команда NET DIAG ініціює низькорівневий діагностичний тест між двома комп'ютерами в мережі. Для цієї мети NET може працювати або як клієнт діагностики, або як її сервер. При запуску команди NET DIAG система спочатку намагається виявити в мережі сервер діагностики. Якщо ця спроба закінчується невдачею, система сама починає виконувати функції сервера. Якщо в системі встановлені протоколи IPX і NetBIOS (TCP/IP або NetBEUI), система запитує в користувача, для якого з протоколів варто виконати діагностичний тест.

Коли система виявляє в мережі сервер, вона передає серію повідомлень сесії NetBIOS чи SAP-повідомлень протоколу IPX і вивчає відповіді, що надходять від сервера. Протягом тесту NetBIOS клієнт установлює із сервером з'єднання TCP чи сесію NetBEUI, а потім починає відправляти повідомлення сесії, що містять тестові дані. У випадку тесту IPX клієнт передає широкомовні повідомлення SAP і приймає відгук від сервера. Після цього клієнт може передавати серверу односпрямовані пакети SAP, що містять тестові повідомлення.

Команда NET DIAG перевіряє працездатність усього стека протоколів і може допомогти виявити проблему у певному сервісі чи протоколі. Наприклад, якщо дві системи можуть успішно обмінюватися повідомленнями PING, але тест NET DIAG між двома машинами не проходить, то можна зробити висновок, що проблема існує десь вище мережевого рівня моделі OSI.

4.1.4 NET START і NET STOP

Команди NET START і NET STOP використовуються для запуску і зупинення мережевих сервісів у даній системі. В ОС Windows можна вико-

ристовувати ці команди, щоб вибрати, які з засобів переадресації варто завантажити за допомогою синтаксису, окремі елементи якого описані нижче.

NET START [BASIC] [NWREDIR] [WORKSTATION] [NETBIND] [NETBEUI] [NWLINK] [/LIST] [/YES] [/VERBOSE]

- BASIC. Запуск базового засобу переадресації.
- NWREDIR. Запуск засобу переадресації Microsoft Client for NetWare Networks (Клієнт Microsoft для мереж NetWare).
- WORKSTATION. Запуск стандартного засобу переадресації.
- NETBIND. Прив'язка протоколів до драйверів мережевих адаптерів.
- NETBEUI. Запуск інтерфейсу NetBIOS.
- NWLINK. Запуск IPX/SPX-сумісного інтерфейсу.
- /LIST. Список сервісів, які виконуються.
- /YES. Виконання команди без попереднього запиту даних чи підтвердьжень.
- /VERBOSE. Виведення на екран інформації про драйвери пристроїв і сервіси по мірі завантаження.

За замовчуванням Windows 98 завантажує повний набір засобів переадресації робочої станції, що забезпечує доступ до доменів і робочих груп мережі. Проте операційна система також включає базовий набір засобів переадресації, який можна використовувати для базових можливостей мережевої взаємодії при мінімумі системних ресурсів. Базовий набір засобів переадресації дозволяє підключатися до робочої групи і здійснювати доступ до ресурсів спільного використання, але не надає можливості зареєструватися в домені Windows NT/2000/ XP/2003/Vista.

У ситуаціях, коли елементи системи функціонують неправильно, наприклад, у випадку відсутності можливості завантажити GUI, можна запустити мережевого клієнта реального режиму, що входить до Windows 98, використовуючи команди NET START BASIC чи NET START WORKSTATION. Ці команди завантажують драйвер NDI 2.0 для мережевого адаптера і драйвери встановлених протоколів, а потім пов'язують драйвери із менеджером протоколів.

Після того як засіб переадресації цілком завантажено, система реєструє користувача в робочій групі чи домені за замовчуванням і запитує пароль. Потім за допомогою команди NET USE можна підключати мережеві диски і здійснювати до них доступ або виконувати інші команди, що підтримують мережеві функції, такі як NET VIEW, що служить для від ображення ресурсів, доступних у мережі, чи NET DIAG – для перевірки мережевої взаємодії. Після того як сервіси запущені, їх можна зупиняти, використовуючи команду NET STOP з тими ж параметрами, що і для запуску сервісів, наприклад, NET STOP WORKSTATION, але тільки поза Windows GUI. Неможливо виконати команду NET STOP у сеансі DOS.

У системах Windows NT можна використовувати команди NET START і NET STOP для запуску і зупинки будь-якого сервісу, запущеного

на ПК, чи використовувати NET PAUSE і NET CONTINUE для тимчасового припинення і продовження роботи сервісу. Введення з командного рядка команди NET START відображає список працюючих у даний момент сервісів, такий як наведено нижче.

These Windows NT services are started: Alerter
Computer Browser Content Index
DHCP Client
Eventlog
IIS Admin Service License Logging Service
Messenger MSDTC Net Logon
NT LM Security Support Provider Plug and Play
Print Server for Macintosh Protected Storage
Remote Procedure Call (RPC) Locator Remote Procedure Call (RPC) Service Server , Spooler
Task Scheduler TCP/IP NetBIOS Helper Workstation
World Wide Web Publishing Service The command completed successfully.

Дія команди NET START без параметрів у системах Windows NT/2000, Windows XP/2003/Vista відрізняється. У системі NT/2000 вона носить лише інформативний характер, а в Windows 98 запускає стандартний засіб переадресації NETSESSION

У Windows NT/2000/XP/2003/Vista можна заблокувати обліковий запис користувача через утиліту User Manager чи через діалогове вікно властивостей об'єкта користувача, і в такий спосіб запобігти можливості реєстрації користувача в мережі. Однак ця міра не робить миттєвого ефекту і вступає в дію тільки з того моменту, коли користувач спробує зареєструватися в мережі у черговий раз. Якщо необхідно негайно відключити користувача від системи, можна використовувати Windows Server Manager чи Computer Management Console, або виконати NET SESSION з командного рядка.

Запуск NET SESSION без параметрів відображає список активних у даній системі сесій, подібно наведеному нижче.

Computer	User name	Client Type	Opens	Idle time
\\CZ2	Administrator	Windows NT 1381	5	00:14:51
WCZ3	JDOE	Windows 4.0	0	00:00:08
WCZ5	CRAIGZ	Windows 4.0	0	06:02:51

The command completed successfully.

Щоб припинити сесію негайно, варто використовувати команду NET SESSION з таким синтаксисом:

NET SESSION [\\ім'я_комп'ютера] /DELETE

Коли в командному рядку вказується NetBIOS-ім'я комп'ютера, NET SESSION негайно припиняє всі сесії цього комп'ютера з даною системою і закриває усі відкриті файли. Якщо ім'я комп'ютера не вказане, NET SESSION припиняє всі сесії з усіма комп'ютерами.

4.1.5 Інспектор мережі

Net Watcher (Інспектор мережі) – це утиліта, включена в Windows, яка дозволяє відслідковувати користувачів мережі, підключених до комп'ютера, ресурси спільного використання, до яких вони в даний момент здійснюють доступ, і файли, відкриті користувачами. Також можна відключати користувачів від ресурсів спільного використання, примусово закривати файли відкриті користувачами і створювати або видаляти доступні ресурси. Net Watcher як правило застосовується для визначення, хто з користувачів у даний момент здійснює доступ до ресурсів спільного використання і файлів даного комп'ютера. Однак з погляду мережевого адміністрування краща можливість цього додатка полягає в тому, що він дозволяє з'єднуватися з іншими комп'ютерами в мережі і виконувати на них віддалені дії.

4.1.5.1 З'єднання з віддаленою системою

Net Watcher має форму виконуваного файлу Netwatch.exe та установлюється за замовчуванням разом з операційною системою Windows. Після запуску Net Watcher програма відображає з'єднання з ПК, які відкриті в даний момент. Щоб відстежити активність іншої робочої станції Windows у мережі, потрібно вибрати з меню Керування (Administer) команду Вибрати сервер (Choose Server) і вказати NetBIOS-ім'я чи IP-адресу комп'ютера, моніторинг якого планується здійснювати.

Щоб з'єднатися з іншою системою Windows за допомогою Net Watcher необхідно, щоб для неї було дозволено віддалене керування. Щоб його дозволити, користувач за іншим ПК повинен відкрити панель керування паролями і на вкладці Remote Administration (Віддалене керування) установити прапорець Enabled Remote Administration of This Server (Дозволити віддалене керування цим сервером), а також задати пароль, що буде використовуватися для підключення до робочої станції.

Для систем, що містять важливі дані, бажано використовувати досить складний пароль, тому що користувач із привілеями віддаленого керування може одержати доступ до усіх дисків системи і віддавати файлові ресурси до спільного користування без жодних обмежень.

Коли дозволяється віддалене керування, Windows створює два адміністративних поділюваних ресурси, зазначених нижче.

- *ADMI$*. Забезпечує адміністраторам доступ до файлової системи навіть коли диски не надані в спільне використання.
- *IPC$*. Забезпечує канал міжпроцесної взаємодії (IPC) між комп'ютером користувача і комп'ютером адміністратора.

Ці ресурси спільного використання дозволяють взаємодіяти з віддаленою системою і спостерігати за її мережевою активністю.

Можливість віддаленого керування в Windows 98 – це не те ж саме, що сервіс Remote Registry (віддалений реєстр), що дозволяє змінювати установлення в реєстрі інших систем мережі. Віддалене керування можна до-

зволити для будь-якої системи Windows 98, у той час як сервіс Remote Registry вимагає керування доступом на рівні користувачів і наявності в мережі системи Windows NT/2000/ XP/2003/Vista.

4.1.5.2 Використання вікна підключень

Під час з'єднання з іншою системою за допомогою програми Net Watcher, що установлюється з Windows, програма виводить вікно Connections (Підключення), яке містить список користувачів і комп'ютерів, що здійснюють доступ до ресурсів спільного використання системи. У лівій панелі виводиться кількість спільних ресурсів і файлів, відкритих кожним користувачем, у той час як у правій панелі вказуються відкриті файли для кожного з ресурсів спільного використання. Можна відключити користувача від комп'ютера (так саме як і від будь-якого спільного ресурсу чи файлу, до якого користувач здійснює доступ), виділивши його ім'я і вибравши з меню Administer (Керування) команду Disconnect User (Відключити користувача).

Як засіб забезпечення безпеки, Net Watcher дозволяє перевіряти мережу на предмет неавторизованого доступу до певних систем і ресурсів спільного використання і вживати заходів для запобігання повторному втручанню. Коли виявляється, що хто-небудь здійснює неавторизований доступ до ресурсу спільного використання, то цього користувача можна негайно відключити від машини, а потім переключитися у вікно Shared Folders (Загальні папки), щоб змінити пароль чи дозволи для спільного ресурсу.

Відключення користувача від системи є радикальним кроком у випадку якщо користувач має відкриті файли. З'єднання розривається без попередження користувача, що може призвести до втрати даних.

4.1.5.3 Використання вікна загальних папок

Два інших вікна програми Net Watcher відображають ту ж саму інформацію, але в іншому форматі. У вікні Shared Folder(s) (Загальні папки) вказано всі диски системи, надані в спільне використання, комп'ютери, підключені до них, і файли, відкриті на кожному з комп'ютерів. З цього вікна можна створювати і видаляти ресурси спільного використання на віддаленій системі, а також змінювати властивості існуючих спільних ресурсів.

Щоб створити новий ресурс спільного використання, слід з меню Administer (Керування) вибрати команду Add shared folder (Зробити папку загальною) і вибрати в діалоговому вікні Browse for Folder (Уведення шляху) бажаний диск або каталог. У цьому діалоговому вікні відображаються існуючі на комп'ютері ресурси спільного використання, а також адміністративні спільні ресурси, подані буквою диска, після якої стоїть символ долара (такий як $). Як кореневий каталог для нового ресурсу спільного використання необхідно вибрати один з цих адміністративних спільних ресурсів чи його підкаталогів. Після того як вибір зроблений, з'явиться стан-

дартне діалогове вікно створення загального ресурсу (у якому можна вказати ім'я для ресурсу спільного використання), де можна задати тип доступу, наданого користувачам, і пароль.

Також можна змінювати пароль для доступу до ресурсу або ім'я самого ресурсу спільного використання, вказавши його в списку і вибравши з меню Administer (Керування) команду Shared Folder Properties (Властивості загальної папки). У випадку несанкціонованого доступу до ресурсу можна навіть видалити повністю ресурс спільного використання, щоб запобігти доступу до нього користувачів.

4.1.5.4 Використання вікна відкритих файлів

У вікні Open Files (Відкриті файли) вказуються імена файлів, що знаходяться у використанні, і користувачі, які працюють з ними.

З цього вікна можна закрити окремі файли (замість повного відключення користувача від системи), вибравши у меню Administer (Керування) команду Close File (Закрити файл). Наприклад, файл може бути не доступним через те, що користувач залишив його відкритим і відійшов від свого комп'ютера, тоді цей файл можна закрити, не перериваючи роботи інших користувачів.

4.1.5.5 Спостереження за мережевою активністю в Windows NT/2000/ XP/2003/Vista

Windows NT Server Resource Kit включає Net Watch, свою власну версію програми Net Watcher (Інспектор мережі), що використовує інший ін.-терфейс, але виконує всі ті ж задачі, що і Net Watcher.

Замість трьох різних вікон, що виводить Net Watcher, Net Watch відображає загальні ресурси, підключення і відкриті файли у вигляді одного ієрархічного дерева, і відключати користувачів, і закривати файли можна за допомогою контекстних меню. Такі ж функції забезпечує утиліта Server Manager, яка включена до Windows NT.

4.1.5.6 Утиліти Server Manager для Windows NT

У Windows 2000 еквівалентні функціональні можливості можуть бути знайдені в консолі Computer Management. Панелі Shares, Sessions і Open Files дозволяють переглядати мережеві з'єднання будь-якої системи в мережі так само, як Server Manager і Net Watcher.

4.1.6 Web Administrator

Web Administrator – це доповнення до сервера Інтернету від Microsoft, що дозволяє керувати багатьма елементами системи Windows NT 4.0 Server за допомогою будь-якого Web-браузера, сумісного з мовою Java. Доступний для вільного завантаження з Web-сайту Microsoft за адресою www.microsoft.com/ntserver/nts/downloads/management/NTSWebAdmin, цей

програмний продукт після установлення створює підкаталог \NTADMIN на Web-сайті, який підтримується системою NT Server. Якщо в браузері вказати цей каталог, то з'явиться основна сторінка програми Web Administrator.

З цього вікна можна виконувати багато завдань, відмінних від тих, що вирішуються за допомогою вбудованих програм адміністрування: Control Panel, Server Manager, User Manager, Performance Monitor та інших утиліт. Задачі, що дозволяє вирішувати Web Administrator, вказані нижче.

– Керування локальними і доменними обліковими записами користувачів, груп і комп'ютерів.
– Керування драйверами пристроїв, встановленими в системі.
– Перегляд журналу реєстрації подій у системі.
– Керування дозволами доступу до загальних ресурсів і файлової системи.
– Відправлення повідомлень користувачам, що зареєструвалися на сервері.
– Віддалене перезавантаження сервера.
– Керування чергами друку і їхнім змістом.
– Запуск, зупинка і припинення роботи сервісів.
– Моніторинг сеансів і відключення користувачів.
– Перегляд інформації про стан сервера і статистики продуктивності.

Web Administrator використовує Java для емуляції елементів керування, що знаходяться в стандартних додатках Windows. Повністю присутня велика частина функціональних можливостей оригінальних програм. За замовчуванням програма інсталяції утиліти Web Administrator встановлює IIS-доступ, що дозволяє звертатись до сайту тільки Web-браузеру, запущеному на самому сервері. Можна змінити цей дозвіл так, щоб тільки певні користувачі чи комп'ютери з зазначеними IP-адресами мали доступ до Web Administrator.

Утиліта Web Administrator є інструментом для керування мережами, яку використовують кілька операційних систем, тому що забезпечує адміністративний доступ до сервера з будь-якого комп'ютера, який підтримує браузер. Незважаючи на те, що багато службових засобів Windows можуть виконувати свої функції з кожної із систем у мережі, Web Administrator дозволяє персоналу, який підтримує функціонування мережі, працювати з іншої операційної системи, такої як Windows, Macintosh чи UNIX, щоб мати доступ до функцій, які властиві Windows.

4.1.7 NetMeeting

Microsoft NetMeeting – це програмний засіб для створення конференцій і колективної роботи, призначений для роботи через Інтернет, але він також може зробити велику послугу адміністратору мережі. NetMeeting є частиною повної установки Internet Explorer, але крім цього програма також доступна окремо у вигляді версій для Windows.

Незважаючи на те, що користувачі Інтернету в основному мають справу з можливостями NetMeeting, спрямованими на створення аудіо- і відеоконференцій, адміністратори мережі можуть використовувати можливості спільної роботи як гарне рішення для забезпечення технічної підтримки без фізичного доступу до місця розташування користувача. Крім аудіо- і відеоконференцій NetMeeting включає можливість ведення бесіди («чат») у текстовому режимі і демонстраційну дошку (електронна дошка білого кольору, на якій можна писати кольоровими маркерами з одночасним поданням інформації на екрані комп'ютера), а також колективну роботу в окремому додатку.

Наприклад, якщо користувач має проблему з додатком, він може надіслати запит у «довідковий стіл» служби підтримки й установити з'єднання з адміністратором за допомогою NetMeeting. Коли користувач робить у рамках NetMeeting додаток загальним, адміністратор може взяти контроль над ним, щоб продемонструвати виконання певної процедури. У будь-який момент часу тільки один користувач може мати контроль над додатком, але користувач, що запросив допомогу, може бачити дії адміністратора (натискання клавіш), і в такий спосіб має можливість вивчати інтерактивний додаток. Так само адміністратор здатний побачити, яким чином користувач намагається виконати задачу і що він робить неправильно.

Інша можливість NetMeeting називається «загальний доступ до робочого столу», вона дозволяє віддаленому користувачу одержати повний контроль над комп'ютером. Адміністратори можуть скористатися цією можливістю для віддаленого конфігурування системи, установлення програмного забезпечення і навіть для запуску додатків.

4.2 Утиліти TCP/IP

TCP/IP став найпоширенішим стеком протоколів у мережевій індустрії. Багато задач адміністрування мережі і виявлення несправностей передбачають роботу з різними елементами цих протоколів. Оскільки практично усі комп'ютерні платформи підтримують TCP/IP, його основні службові засоби були перенесені на велику кількість різних операційних систем. Розглянемо деякі з цих засобів, які більшою мірою корисні для адміністратора мережі.

4.2.1 PING

Утиліта PING є найпоширенішим засобом діагностики TCP/IP і включена практично в кожну реалізацію протоколів TCP/IP. У більшості випадків це утиліта командного рядка, хоча існують кілька графічних версій, а також версії на базі меню. Усі вони виконують одні й ті ж самі задачі. Основна функція PING полягає у відправленні повідомлення іншій TCP/IP-системі у мережі, щоб визначити, чи правильно працює стек протоколів аж

до мережевого рівня. Оскільки стек протоколів TCP/IP функціонує однаково у всіх системах, то можна використовувати програму для перевірки з'єднання між двома будь-якими комп'ютерами незалежно від процесорної платформи чи операційної системи.

Усі Windows-системи встановлюють програму PING, призначену для роботи з командного рядка, як частину свого стека протоколів TCP/IP. Вона називається ping.exe і розміщується в системному каталозі, такому як C:\Windows. Схожим чином усі командні процесори в різних варіантах UNIX підтримують команду PING. Novell NetWare включає утиліту ping.nlm з інтерфейсом на основі меню, яка запускається на сервері, а також реалізацію для командного рядка сервера з ім'ям Tping.nlm.

PING працює передаючи послідовність повідомлень Echo Request за зазначеною IP-адресою за допомогою протоколу ICMP (Internet Control Message Protocol). Коли система, що використовує цю IP-адресу, приймає повідомлення, вона створює повідомлення Echo Reply у відповідь на кожен запит Echo Request і передає його назад відправнику. ICMP є протоколом з декількома десятками типів повідомлень, що виконують різні функції діагностики і передачі звітів про помилки. Повідомлення ICMP переносяться безпосередньо усередині IP-дейтаграм. Протокол транспортного рівня не задіюється, тому успішне завершення тесту PING говорить про те, що стек протоколів нижче мережевого рівня функціонує правильно. Якщо система, яка відправила повідомлення Echo Request, не одержує на них відгуків, то означає, що не налагоджене приймання/відправлення або мережеве з'єднанням між системою відправника і отримувача.

У випадку, якщо програма PING реалізована у вигляді утиліти командного рядка, для виконання тесту PING варто використовувати такий синтаксис:

PING *призначення*,

де *призначення* є змінною, яку доцільно замінити ім'ям або IP-адресою іншої системи в мережі. Система призначення може бути ідентифікована її IP-адресою чи ім'ям у випадку, якщо наявний відповідний механізм, що дозволяє такі імена. Це означає, що можна використовувати хост-ім'я для вказання системи призначення, якщо існує DNS-сервер або файл HOSTS з відповідними налаштовуваннями. У мережах Windows також можна використовувати NetBIOS-ім'я, покладаючись на будь-який стандартний механізм для їх перетворення на IP-адреси, такий як сервери WINS, широкомовні передачі чи файл LMHOSTS.

Вікно виведення результатів виконання команди PING виглядає так:

```
Pinging cz3 [192.168.2.3] with 32 bytes of data:
Reply from 192.168.2.3: bytes2 time=lms TTL_8 Reply from 192.168.2.3: bytes2 time<10ms TTL_8
Reply from 192.168.2.3: bytes2 time=lms TTL_8 Reply from 192.168.2.3: bytes2 time<10ms TTL_8
Ping statistics for 192.168.2.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Оскільки більшість реалізацій PING відображають IP-адресу, визначену на основі імені системи або зазначену в командному рядку, то програма PING також є швидким і простим засобом для того, щоб визначити IP-адресу потрібної системи.

Програма відображає рядок результатів для кожного відправленого повідомлення Echo Request, за замовчуванням вказуючи IP-адресу отримувача, кількість байтів, переданих у кожному повідомленні, кількість часу, що пройшло між передачею повідомлення й одержанням відгуку, а також TTL (час життя) пакету. TTL – це максимальна кількість послідовних маршрутизаторів, через які може бути переданий пакет.

PING має інше діагностичне застосування крім визначення чи існує система і чи працює вона. Якщо тест PING з використанням IP-адреси проходить успішно, а PING із вказанням імені системи закінчується невдачею, то проблема полягає в збої, що виникає в процесі визначення IP-адреси. При спробі взаємодії з Інтернет-сайтом це свідчить про те, що проблема або з конфігурацією DNS-сервера, що задана на робочій станції, або із самим DNS-сервером. Якщо тест PING для систем у локальній мережі проходить успішно, а для систем з Інтернету закінчується невдачею, то проблема або з установленням шлюзу за замовчуванням у конфігурації робочої станції, або в з'єднанні з Інтернетом.

Відправлення команди PING за адресою зворотного зв'язку системи (127.0.0.1) з'ясовує роботоздатність стека протоколів TCP/IP, але не є адекватним способом перевірити роботу мережевого адаптера, тому що трафік, відправлений за цією адресою, поширюється вниз по стеку протоколів тільки до мережевого рівня і повертається назад. До мережевого адаптера сигнал не потрапляє.

У більшості реалізацій PING дозволяє задавати в командному рядку додаткові параметри, щоб змінити розмір і кількість повідомлень Echo Request, переданих однією командою PING, а також робочі характеристики. У програмі ping.exe для Windows, наприклад, є такі параметри:

PING [-t] [-a] [n число] [-1 розмір] [-f] [-i TTL] [-v TOS] [-r число] [-s число] [[-j список_вузлів] | [-k ,список_вузлів]] [-w таймаут] [-R] [-S] [-4] [-6] станція_призначення:

- -t Визначає відправлення пакетів на зазначений вузол до команди переривання від користувача (комбінація клавіш <Ctrl>+<C>);
- -a Визначає IP-адресу за іменем вузла;
- -n число. Указує кількість повідомлень Echo Request, які потрібно відправити;
- -1 розмір. Задає розмір повідомлень Echo Request, що відправляються;
- -f. Установлює прапорець, що забороняє фрагментацію пакетів Echo Request;
- -i TTL. Задає значення TTL для пакетів Echo Request;

- -v TOS. Задає тип служби (TOS, Type of Service) для пакетів Echo Request;
- -r число. Робить запис IP-адрес маршрутизаторів для зазначеного числа транзитів;
- -s число. Робить запис тимчасових оцінок проходження маршрути заторів для зазначеного числа транзитів;
- -j список_вузлів. Задає неповний список маршрутизаторів (вільний вибір маршруту), через які повинні пройти пакети;
- -k список_вузлів. Задає повний список маршрутизаторів (примусовий маршрут), через які повинні пройти пакети;
- -w таймаут. Інтервал чекання кожної відповіді в мілісекундах;
- -R. Використовувати заголовки для діагностики зворотнього маршруту (тільки IPv6);
- -S. Джерело адреси (тільки IPv6);
- -4. Застосувати IPv4;
- -6. Застосувати IPv6.

Існує велика кількість різних застосувань для цих параметрів, що можуть допомогти керувати мережею і виявляти проблеми. Наприклад, створивши пакети Echo Request більшого, ніж звичайно, розміру і відправивши більшу їхню кількість (чи відправляючи їх безупинно), можна емулювати у мережі трафік користувача, щоб перевірити її можливість залишатися стабільною при великому завантаженні. Також можна порівняти продуктивність різних маршрутів через мережу (чи через Інтернет), задавши IP-адреси маршрутизаторів, через які повинні пройти пакети Echo Request, щоб досягти свого місця призначення. Параметр – j забезпечує вільний вибір маршруту, що наказує пакетам використовувати маршрутизатори, IP-адреси яких задані, але також можуть застосовуватися й інші маршрутизатори. Параметр -k забезпечує примусовий маршрут, при якому необхідно вказати адресу кожного маршрутизатора, який повинен використовуватися, щоб пакет зміг досягти місця призначення.

4.2.2 Traceroute

Traceroute – це утиліта командного рядка, яку включено в більшість реалізацій стеків TCP/IP, хоча іноді вона носить інше ім’я. У системах UNIX команда називається traceroute, а реалізація для Windows з такими ж функціональними можливостями називається Tracert.exe. Призначенням цього програмного засобу є відображення маршруту, який проходять IP-пакети для досягнення системи призначення. Коли програма запускається з вказанням імені або IP-адреси системи призначення як параметра командного рядка, то результат, виведений на екран, буде виглядати приблизно так:

```
Tracing routeto zacker.com [192.41.15.74] over a maximum of 30 hops:
1    254 ms    194 ms    162 ms    qrvl-67.epix.net [199.224.67.3]
2    151 ms    135 ms    154 ms    qrvl.epix.net [199.224.67.1]
```

```
3    163 ms    150 ms    173 ms    svcrO-7b.epix.net [199.224.103.125]
4    136 ms    160 ms    164 ms    router05.epix.net [216.37.155.162]
5    161 ms    145 ms    170 ms    cpbgOl-7.epix.net [199.224.88.62]
6    165 ms    149 ms    164 ms    Seriall.ph.ALTER.NET [157.130.7.213]
7    182 ms    242 ms    169 ms    161.ATM2.ALTER.NET [146.188.162.118]
8    178 ms    149 ms    1839 ms   294.ATM7.ALTER.NET [146.188.160.126]
9    168 ms    147 ms    155 ms    192.ATM10.ALTER.NET [146.188.160.93]
10   260 ms    150 ms    176 ms    uu.iadl.verio.net [137.39.23.22]
11   163 ms    175 ms    166 ms    iad3.dcaO.verio.net [129.250.2.62]
12   235 ms    243 ms    244 ms    dcaO.pao5.verio.net [129.250.2.245]
13   224 ms    249 ms    255 ms    p4-01.us.bb.verio.net [129.250.2.74]
14   406 ms    272 ms    265 ms    pao6.pvuO.verio.net [129.250.3.26]
15   267 ms    250 ms    271 ms    puO.vwh.verio.net [129.250.16.14]
16   257ms     270ms     278ms     zacker.com [192.41.15.74]
Trace complete.
```

Кожен запис у трасуванні позначає маршрутизатор, який обробляв пакети, створені програмою traceroute, на шляху до їх місця призначення. У даному випадку пакетам знадобилося 16 транзитів, щоб досягти сервера zacker.com. Тризначні числа в кожному записі визначають час проходження пакета до даного маршрутизатора і назад у мілісекундах, за ними вказано доменне ім'я маршрутизатора і його IP-адресу. У трасуванні до місця призначення, яке розташоване в Інтернеті, значення часу переходу пакета туди і назад порівняно великі і можуть надати інформацію про магістральні мережі, які використовує постачальник послуг Інтернету (у даному випадку alter.net), і географію маршруту, по якому передається трафік. У приватній мережі команду Traceroute можна використовувати для визначення шляху через маршрутизатори, якими рухається локальний трафік, що дозволяє виконати аналіз щодо того, яким чином можна краще розподілити трафік через мережу.

Більшість реалізацій traceroute працюють, передаючи такий самий тип ICMP-повідомлень Echo Request, як утиліта PING, хоча деякі версії використовують за замовчуванням пакети UDP. Єдине розходження полягає в самих повідомленнях, де програма traceroute змінює значення полів TTL для кожної послідовності з трьох пакетів. Поле TTL є захисним механізмом, що запобігає нескінченній циркуляції IP-пакетів у мережі. У кожному пакеті, що обробляється, маршрутизатор зменшує значення поля TTL на одиницю. Якщо значення поля TTL пакета досягає 0, маршрутизатор відкидає такий пакет і повертає тій системі, яка його відправила, ICMP-повідомлення про помилку «Time to Live Exceeded in Transit».

У першій послідовності пакетів traceroute значення TTL дорівнює 1. Таким чином, перший маршрутизатор, що одержав пакети, відкидає їх і повертає назад джерелу повідомлення про помилку. Обчисливши інтервал часу між передачею повідомлення і появою пов'язаної з ним помилки, traceroute одержує час проходження пакета туди і назад, а потім використовує IP-адресу джерела повідомлення про помилку для ідентифікації мар-

шрутизатора. В другій послідовності повідомлень значення TTL дорівнює 2, тому пакет досягає другого маршрутизатора перш, ніж буде відкинутий. Третя послідовність пакетів має значення TTL рівне 3, і так далі, поки повідомлення не досягнуть системи призначення.

Важливо розуміти, що, незважаючи на можливу користь цього засобу, в інформацію, що він надає, закладена певна неточність. Просто той факт, що пакет, переданий прямо зараз, досяг місця призначення, пройшовши по певному маршруту, не означає, що пакет, переданий хвилиною пізніше, потрапить у те ж місце призначення, по такому ж маршруту. Мережі (і особливо Інтернет) мінливі і маршрутизатори розроблені для того, щоб автоматично враховувати виникаючі зміни. Маршрут, яким йдуть до свого місця призначення пакети traceroute, може змінюватися навіть усередині процесу трасування, тому цілком можливо, що послідовність маршрутизаторів, яка відображається програмою, буде складена з двох чи більш різних шляхів до місця призначення через зміни, що відбулися в мережі. У приватній мережі такий випадок менш ймовірний, але все ж таки можливий.

4.2.3 Route

Таблиця маршрутизації є життєво важливою частиною мережевого стека будь-якої системи TCP/IP, навіть тієї, що не виконує функції маршрутизатора. Система використовує таблицю маршрутизації, щоб визначити, як варто передавати кожен пакет. Програма Route.exe у Windows і команда route, включена в більшість версій UNIX, дозволяє переглядати таблицю маршрутизації і додавати чи видаляти запис в ній.

4.2.4 Netstat

Netstat є утилітою командного рядка, яка відображає статистику мережевого трафіка для різних протоколів TCP/IP і, залежно від платформи, може також виводити на екран іншу інформацію. Більшість варіантів UNIX підтримують команду NETSTAT, а операційні системи Windows включають програму Netstat.exe, яка за замовчуванням установлюється разом із стеком TCP/IP. Параметри командного рядка для NETSTAT у різних реалізаціях можуть різнитися, але одним з основних є параметр -s, що відображає статистику для кожного з основних протоколів TCP/IP, як показано нижче:

```
                IP Statistics
Packets Received                   = 130898
Received Header Errors             = 0
Received Address Errors            = 19
Datagrams Forwarded                = 0
Unknown Protocols Received         = 0
Received Packets Discarded         = 0
Received Packets Delivered         = 130898
Output Request                     = 152294
```

Routing Discards	= 0
Discarded Output Packets	= 0
Output Packet No Route	= 0
Reassembly Required	= 0
Reassembly Successful	= 0
Reassembly Failures	=0
Datagrams Successfully'Fragmented	=0
Datagrams Failing Fragmentation	= 0
Fragments Created	= 0

ICMP Statistics	Received	Sent
Messages	499	683
Errors	44	0
Destination Unreachable	0	154
Time Exceeded	414	0
Parameter Problems	0	0
Source Quenchs	0	0
Redirects	0	0
Echos	1	522
Echo Replies	27	1
Timestamps	0	0
Timestamps Replies	0	0
Address Masks	0	0
Address Mask Replies	0	0

TCP Statistics	
Active Opens	= 1893
Passive Opens	= 12
Failed Connection Attempts	= 37
Reset Connections	= 657
Current Connections	= 0
Segments Received	= 117508
Segments Sent	= 142099
Segments Retransmitted	= 378

UDP Statistics	
Datagrams Received	= 12399
No Ports	= 943
Receive Errors	= 0
Datagrams Sent	= 9129

Незважаючи на загальну кількість пакетів, що були прийняті і передані кожним протоколом, NETSTAT надає різноманітну інформацію про збійні ситуації й інші процеси, що може допомогти виявити проблеми мережевої взаємодії на різних рівнях моделі OSI. Версія NETSTAT для Windows також здатна відображати статистику Ethernet (при використанні параметра -e), що може допомогти ізолювати проблеми з мережевим устаткуванням. Інформація, відображувана NETSTAT, наведена нижче.

Interface Statistics	Received	Sent
Bytes	44483612	20434045
Unicast packets	94653	92824
Non-unicast packets	4543	743
Discards	0	0
Errors	0	0
Unknown protocols	15452	

Під час запуску з параметром -e програма Netstat.exe відображає інформацію про з'єднання TCP, які активні у даний момент на комп'ютері, і сервіси UDP, що очікують вхідних даних, як показано нижче.

Active Connections

Proto	Local Address	Foreign Adress	State
TCP	cz5:1044	CZ5:0	LISTENING
TCP	cz5:1025	CZ5:0	LISTENING
TCP	cz5:1025	CZl:nbsession	ESTABLISHED
TCP	cz5:137	CZ5:0	LISTENING
TCP	cz5:138	CZ5:0	LISTENING
TCP	cz5:nbsession	CZ5:0	LISTENING
TCP	cz5:nbsession	CZ3:1531	ESTABLISHED
TCP	cz5:2521	netsurge.com:pop3	TIME_WAIT
UDP	cz5:1044	**	
UDP	cz5:nbname		
UDP	cz5:nbdataqram		

Також можливо вивести статистику мережевого трафіка для протоколів верхніх рівнів, таких як Server Message Blocks (SMB), використовуючи команду NET STATISTICS.

4.2.5 Nslookup

Nslookup є утилітою, яка дозволяє відправляти запити безпосередньо певному DNS-сервера, щоб визначити ім'я з IP-адреси або запросити іншу інформацію. На відміну від інших методів визначення імен, таких як використання PING, Nslookup дозволяє вказати, який із серверів одержить команди, що дає можливість визначити, чи правильно працює DNS-сервер і чи містить він правильні дані. Спочатку розроблена для систем UNIX, програма Nslookup.exe також включена до мережевих клієнтів для операційних систем Windows NT/2000/XP/2003/Vista. Також доступні реалізації Nslookup від сторонніх виробників, наприклад програма з графічним інтерфейсом, включена до CyberKit.

Nslookup.exe може бути запущена в інтерактивному і неінтерактивному режимі. Щоб передати окремий запит, можна використовувати неінтерактивний режим, застосовуючи в командному рядку такий синтаксис:

Nslookup ім'я_вузла ім'я_сервера.

Замість змінної ім'я_вузла варто вказати доменне ім'я або IP-адресу, які потрібно встановити, а змінну ім'я_сервера замінити на ім'я або IP-ад-

ресу DNS-сервера, якому цей запит треба надіслати. Якщо опустити параметр ім'я_сервера, програма використовує DNS-сервер за замовчуванням. Результат роботи програми в неінтерактивному режимі в Windows виглядає в такий спосіб:

```
Server: nsl.secure.net Address: 192.41.1.10
Name: zacker.com Address: 192.41.15.74
Aliases: www.zacker.com
```

Щоб запустити Nslookup в інтерактивному режимі, слід ввести ім'я програми в командному рядку без вказання параметрів (для використання DNS-сервера за замовчуванням) чи з дефісом на місці змінної ім'я_вузла і наступним за ним ім'ям DNS-сервера, як показано нижче:

```
Nslookup – ім'я_сервера
```

Програма формує запрошення для введення у вигляді кутової дужки (>), після якої можна набирати імена чи адреси, а також велику кількість команд, що змінюють параметри, які використовуються Nslookup для запиту сервера імен. Список команд можна вивести на екран, набравши в рядку запрошення слово help. Для виходу з програми служить комбінація клавіш <Ctrl>+<C>.

4.2.6 Ipconfig

Програма Ipconfig є простою утилітою для відображення конфігураційних параметрів TCP/IP системи. Це особливо корисно, коли для автоматичної конфігурації клієнтів TCP/IP у мережі використовуються сервери DHCP, тому що для користувачів не існує іншого простого способу побачити, які установлення були призначені їх робочим станціям. Усі реалізації UNIX включають команду ipconfig (з довільною конфігурацією інтерфейсу), і системи Windows мають програму командного рядка Ipconfig.exe. У Windows 95/98 також включена утиліта Winipcfg.exe із графічним інтерфейсом, що виконує ті самі функції.

Запуск Ipconfig.exe з параметром /all у системі Windows виводить таку інформацію:

```
Windows 2000 IP Configuration
   Host Name ..........................        : cz2
   Primary DNS Suffix..................        : zacker.com
   Node Type..............................  …        : Hybrid
   IP Routing Enabled..................  .        : No
   WINS Proxy Enabled .................        : No
   DNS Suffix Search List. : zacker.com
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix:
   Description ..........................:    3Com Etherlink III (3C509/3c509b)
   Physical Address.....................:    00-60-97-B0-77-CA
   DHCP Enabled .........................:    Yes
   Autoconfiguration Enabled . . :            Yes
```

```
IP Address.....:   192.168.2.21
Subnet Mask ..... :  255.255.255.0
Default Gateway ..... : 192.168.2.100
DHCP Server ..... : 192.168.2.10
DNS Servers ..... : 199.224.86.15
199.224.86.16
Primary Wins Server ..... : 192.168.2.10
Lease Obtained ..... : Sunday, Feb 06, 2000 10:08:23 PM
Lease Expires..... .. : Tuesday, Feb 09, 2000 10:08:23 PM
```

Ipconfig також можна використовувати, щоб анулювати чи відновлювати використання IP-адреси з сервера DHCP за допомогою параметрів /release і /renew, відповідно.

4.3 Аналізатори мережі

Аналізатор мережі, який іноді називають аналізатором протоколів, є пристроєм, що захоплює переданий по мережі трафік і аналізує його властивості декількома різними способами. Основною функцією аналізатора є декодування і відображення вмісту захоплених у мережі пакетів. Для пакетів програма виводить інформацію, знайдену в кожному з полів кожного протокольного заголовка, а також дані вихідного додатка, отримані як корисні дані пакета. Аналізатори, до того ж, часто надають таку статистику про переданий трафік по мережі, як число пакетів, які використовуються певним протоколом, і кількість трафіка, що згенерований кожною системою в мережі. Аналізатор мережі також є чудовим засобом для навчання. Немає кращого способу познайомитися з мережевими протоколами і їхніми функціями, ніж побачити їх у дії.

Існують дуже різноманітні аналізатори мережі, починаючи з окремих апаратних пристроїв і закінчуючи програмними продуктами. Наприклад, Windows включає додаток Network Monitor, що дозволяє аналізувати мережевий трафік.

По суті, аналізатор мережі – це додаток, запущений на комп'ютері з установленою платою мережевого адаптера. Це пояснює чому ці пристрої можуть або включати апаратне забезпечення, або набувати винятково форми програми. Консультант, що рухається по мережах, може мати потративний комп'ютер із програмним забезпеченням комплексного аналізатора мережі і різних мережевих адаптерів, що підтримують різні мережі, у той час як адміністратору, що обслуговує приватну мережу, краще буде використовувати менш дорогий програмний аналізатор мережі, що підтримує лише даний тип мережі.

Аналізатор мережі працює переключаючи плату мережевого адаптера комп'ютера, на якому він запущений, у невпорядкований режим (promiscuous mode) роботи. Зазвичай мережевий адаптер досліджує адреси призначення в заголовку протоколу канального рівня кожного пакета, що

досягає комп'ютера, і якщо пакет адресований не цьому комп'ютеру, мережевий адаптер ігнорує його. Це запобігає обробці центральним процесором системи тисяч сторонніх пакетів. Однак коли мережевий адаптер переключений у невпорядкований режим роботи, він приймає всі пакети, що приходять з мережі, незалежно від їхньої адреси призначення, і передає їх для обробки програмі аналізатора мережі. Це дозволяє системі аналізувати не тільки трафік, створений системою чи призначений для системи з запущеним програмним забезпеченням аналізатора, але також трафік, яким обмінюються інші системи в мережі.

Коли додаток захоплює з мережі трафік, він зберігає всі пакети в буфері, до якого надалі звертається під час аналізування. Залежно від розміру мережі й інтенсивності переданого трафіку, кількість захоплених даних може бути великою, тому зазвичай варто задавати розмір буфера, щоб контролювати кількість захоплених даних. Також можна застосовувати фільтри, щоб обмежити типи даних, що захоплюються аналізатором.

4.3.1 Фільтрація даних

Через те, що багато мереж передають велику кількість даних, регулювання обсягу даних, які захоплюються і обробляються аналізатором мережі, є важливим елементом. Це керування може бути реалізовано застосуванням фільтрів в процесі захоплення або після нього. Коли мережеві дані захоплюються без обробки, результат може бути незрозумілим, тому що всі пакети, створені різними додатками на численних системах мережі, перемішані разом у хронологічному порядку. Застосування фільтрів змусить програму відображати тільки необхідну інформацію і допоможе зорієнтуватися у величезній кількості доступних даних.

Більшість аналізаторів мережі забезпечують два типи фільтрів.

– Фільтри захоплення. Накладають обмеження на пакети, які аналізатор зчитує у свій буфер.

– Фільтри відображення. Обмежують відображення захоплених пакетів на екрані.

Зазвичай обидва типи фільтрів працюють однаково, єдине розходження між ними полягає в тому, коли вони застосовуються. Можна вибрати, чи варто фільтрувати пакети при зчитуванні їх у буфер аналізатора або захоплювати з мережі всі дані і використовувати фільтри для обмеження виведення цих даних на екран (чи використовувати обидва способи).

Фільтрацію даних в аналізаторі мережі можна здійснювати декількома різними способами, залежно від того, яку інформацію про мережу необхідно одержати. Наприклад, якщо потрібно досліджувати продуктивність певного комп'ютера, можна створити фільтр, що буде захоплювати тільки пакети, створені цим ПК, призначені для нього, чи усі інші. Також можна створити фільтри, засновані на протоколі, який використовується в пакетах, що дозволить, наприклад, захоплювати тільки трафік DNS на виході

чи за зразком, щоб захоплювати тільки пакети, що містять визначений ASCII- чи шістнадцятковий рядок. Комбінуючи ці можливості за допомогою логічних операторів, таких як AND або OR, можна створити спеціалізовані фільтри, що будуть відображати лише необхідну інформацію. Аналізатори мережі можуть використовувати різноманітні інтерфейси і пропонувати додаткові можливості, оскільки фільтрація пакетів відбувається на основі їх розміру або певних умов помилки, але основні функціональні можливості будуть тими ж.

4.3.2 Агенти

Апаратні аналізатори мережі є пересувними і розроблені для підключення до мережі в будь-якій її точці. Програмні реалізації не переміщаються і часто включають механізм (який іноді називають агентом), що дозволяє захоплювати мережевий трафік за допомогою мережевого адаптера іншого комп'ютера. Використовуючи агентів, можна встановити програмний аналізатор на одній машині і за допомогою нього здійснювати підтримку всієї мережі. Агент зазвичай є драйвером чи сервісом, який запущений на робочій станції, котра розташована десь у мережі. Наприклад, усі версії Windows включають Network Monitor Agent, що забезпечує для додатка Network Monitor, запущеного на сервері Windows, можливості віддаленого захоплення трафіка.

Деякі версії Network Monitor, що включені до Windows, обмежені можливістю захоплення тільки того трафіка, який призначений системі, на яку він спрямований або з якої виходить. Іншими словами мережевий адаптер не переключається у невпорядкований режим. Щоб захопити весь мережевий трафік, необхідно використовувати повнофункціональну версію Network Monitor, що включена в програмний пакет Microsoft System Management Server (SMS).

Коли аналізатор мережі запускається на системі з одним мережевим адаптером, додаток за замовчуванням захоплює дані, що приходять на цей інтерфейс. Якщо в системі встановлено більше одного інтерфейсу у вигляді іншої плати мережевого адаптера або модемного з'єднання, можна вибрати інтерфейс, дані якого будуть захоплюватися. Коли аналізатор має можливість застосування агентів, у тому ж діалоговому вікні можна вказати ім'я чи адресу іншого комп'ютера, на якому запущений агент. Потім додаток з'єднується з цим комп'ютером, використовує його мережевий адаптер для захоплення мережевого трафіка і передає його у буфери системи, на якій запущений аналізатор. Однак коли використовується агент, розташований в іншому сегменті мережі, важливо врахувати, що сама передача від агента до аналізатора породжує значний трафік.

4.3.3 Аналіз трафіка

Деякі аналізатори мережі можуть відображати статистику про трафік у мережі в міру його захоплення, як кількість пакетів у секунду, розбитих по робочих станціях. Залежно від продукту, також можливо подання цієї інформації в графічній формі. Цю інформацію можна використовувати для визначення кількості трафіка, який створюється кожною системою мережі чи кожним протоколом.

Використовуючи цей засіб, можна визначити, яка кількість пропускної здатності мережі витрачається певним додатком чи користувачем. Наприклад, якщо відзначено, що робоча станція генерує значну кількість трафіка HTTP, то можна зробити висновок, що на цій станції користувач інтенсивно переглядає Web-сторінки. За допомогою фільтрів захоплення можна конфігурувати аналізатор мережі для відправлення адміністратору аварійних сигналів під час виникнення в мережі певних ситуацій. Деякі продукти можуть генерувати аварійні сигнали, коли трафік певного типу досягає заданого рівня, наприклад, коли в мережі Ethernet виникає занадто велика кількість колізій.

Крім можливості захоплення пакетів з мережі, деякі аналізатори також можуть генерувати їх самі. Можна використовувати аналізатор для імітації трафіка певної інтенсивності, щоб перевірити робочий стан мережі чи устаткування, чутливого до навантаження.

4.3.4 Аналіз протоколів

Після того як захоплений трафік поміщено у буфери аналізатора, можна досліджувати пакети більш детально. У більшості випадків пакети, захоплені протягом періоду захоплення трафіка, відображаються хронологгічно у вигляді таблиці, де вказано найважливіші характеристики кожного пакета, такі як адреси системи призначення і відправника та основний протокол, використаний для створення пакета. При виборі пакета зі списку відображаються додаткові панелі, що містять протокольні заголовки і дані пакета, зазвичай в неопрацьованій і декодованій формі.

Перше застосування для інструмента подібного типу полягає в тому, що можна побачити, які типи трафіка присутні в мережі. Наприклад, якщо мережа використовує канали зв’язку глобальної мережі, що є більш дорогими порівняно з з’єднаннями локальної мережі, можна використовувати аналізатор, щоб захопити трафік, переданий по цих каналах, і переконатися в тому, що їх пропускна здатність не витрачається абияк.

Однією з ознак, за якою можна відрізнити професійні аналізатори мережі від більш дешевих, є кількість підтримуваних програмою протоколів. Щоб правильно декодувати пакет, аналізатор повинен підтримувати всі протоколи, використані для створення цього пакета на всіх рівнях еталонної моделі OSI. Наприклад, типовий аналізатор підтримує Ethernet і, можливо, Token Ring на Канальному рівні, але якщо мережа використовує FDDI чи

ATM, необхідно придбати дорожчий продукт. Це ж саме справедливо і для верхніх рівнів. Практично усі аналізатори підтримують протоколи TCP/IP, а значна кількість також IPX і NetBEUI. Але, перш ніж придбати аналізатор, необхідно переконатися, що він підтримує всі протоколи, які використовуються в мережі. Також варто брати до уваги необхідність модернізації для підтримки майбутніх модифікацій протоколів, таких як IPv6.

Декодуючи пакет, аналізатор здатний інтерпретувати функцію кожного біта і відобразити заголовки різних протоколів у зручному для користувача ієрархічному форматі. Можна розгорнути інформацію для кожного протоколу, щоб досліджувати вміст полів його заголовка.

Аналізатор мережі є потужним інструментом, що може бути легко використаний з метою виявлення проблем у мережі і її підтримки. Коли програма декодує пакет, вона відображає весь його вміст, включаючи інформацію, що може бути секретною. Протокол FTP, наприклад, передає паролі користувача в текстовому вигляді, і вони можуть бути легко прочитані при захопленні пакетів аналізатором мережі. Неавторизований користувач, що запустив аналізатор, може перехопити паролі адміністраторів і одержати доступ до захищених серверів. Це одна з причин, за якою версія Network Monitor, включена до Windows, обмежена можливістю захоплення трафіка локальної системи.

4.3.5 Тестери кабелю

Аналізатор мережі може допомогти в діагностиці багатьох типів мережевих проблем, але він покладається на те, що фізична мережа функціонує правильно. Коли проблема полягає в кабелі, що формує мережу, необхідні різні види пристроїв, що мають назву «тестер кабелю». Тестери кабелю зазвичай являють собою мобільними пристроями, які приєднуються до мережі, щоб виконати різні діагностичні тести провідності мережевого кабелю. Існує широкий вибір пристроїв, що значно відрізняються за вартістю і функціональними можливостями. Прості пристрої доступні за ціною в кілька сотень доларів, у той час як моделі високого рівня можуть коштувати кілька тисяч доларів. Деякі комбіновані тестери можна приєднувати до різних типів мережевого кабелю, таким як неекранована вита пара (UTP), екранована вита пара (STP) і коаксіальний кабель, у той час як інші здатні перевіряти лише один тип кабелю. Для зовсім інших технологій передачі сигналів, таких як оптоволоконний кабель, необхідно окремий пристрій.

Тестери кабелю перевіряють чи відповідає прокладена мережа певному стандарту. Під час прокладення кабелю відповідний фахівець тестує кожен зв’язок, щоб переконатися в правильності його роботи, і перевіряє відсутність проблем, що можуть бути викликані якістю самого кабелю чи природою його установлення. Наприклад, гарний тестер кабелю перевіряє електричний шум, викликаний лампами денного світла або іншим ефектричним устаткуванням (розташованим близько), перехресні завади від сиг-

налів у сусідніх жилах, загасання, викликане надмірно довгими сегментами кабелю чи невідповідною категорією кабелю, короткі замикання й обриви кабелю, подані певним рівнем ємнісного опору.

Крім перевірки життєздатності розводки кабельної мережі, тестери кабелю є гарним засобом для виявлення проблем з кабелем. Наприклад, тестер, що функціонує як рефлектометр, може визначити обрив чи коротке замикання в кабелі, передаючи високочастотний сигнал і вимірюючи кількість часу, що пройшла до того моменту, коли відбитий сигнал повернеться назад. Використовуючи цю техніку, можна визначити, на якій відстані від тестера в кабелі відбувся обрив чи виникла інша несправність. Знаючи, що проблема розташована на відстані, наприклад 20 м, можна уникнути перевірки кожного метра кабелю, що йде до цього місця. Деякі тестери також можуть допомогти визначити маршрут, по якому кабель проходить через стіни чи стелі. Для цього використовується звуковий генератор, що посилає по кабелю сильний сигнал, який може уловити тестер, якщо буде розташований поблизу від кабелю.

Контрольні питання до розділу 4

1. Охарактеризувати можливості та призначення команди NET.
2. Охарактеризувати можливості та призначення команди NET CONFIG.
3. Охарактеризувати можливості та призначення команди NET DIAG.
4. Охарактеризувати можливості та призначення команд NET START і NET STOP.
5. Описати суть роботи та призначення програми-інспектора мережі NET WATCHER.
6. Дати оцінку програми Server Manager.
7. Дати оцінку програми Web Адміністратор.
8. Дати оцінку програми Net Meeting.
9. Дослідити можливості програми PING.
10. Дослідити можливості програми Traceroute.
11. Дослідити можливості програми Route.
12. Дослідити можливості програми Netstat.
13. Дослідити можливості програми Nslookup.
14. Дослідити можливості програми Ipconfig.
15. Обґрунтувати перспективність використання аналізаторів мережі.
16. Описати особливості аналізаторів трафіка.
17. Описати особливості аналізу протоколів.
18. Апаратно-програмні засоби тестування кабелю.
19. Дослідити поняття мережевого керування як попереджувального заходу.

Завдання для студентів заочної форми навчання

Розробити блок-схему комп'ютерної мережі, у якій n робочих станцій, m веб-серверів, h файл-серверів, d серверів вхідної та вихідної пошти, k DNS-серверів, r DHCP-серверів, заданої топології та стандарту передавання. Діапазон IP-адрес для адресації комп'ютерів 192.168.0.74–192.168.0.215. Для кожного комп'ютера вказати можливі типи операційної системи, яка потрібна для коректної роботи, обґрунтувати її вибір. Для всієї мережі підрахувати можливу вартість всього можливого програмного забезпечення, що необхідно для роботи мережі певного призначення. Варіанти завдання видаються викладачем.

У відповіді обґрунтувати вибір та відповідність технології та топології мережі, що розробляється.

№ варіанта	Кількість робочих станцій, n	Кількість веб-серверів, m	Кількість файл-серверів, h	Кількість серверів вхідної та вихідної пошти, d	Кількість DNS-серверів, k	Кількість DHCP-серверів, r	Топологія мережі	Стандарт передавання мережі	Цільове призначення мережі
1.	12	5	3	1	4	2	Шина	FDDI	Навчальна
2.	47	12	7	1	1	2	Зірка	Fast Ethernet	Банківська
3.	45	9	2	1	5	2	Кільце	Gigabit Ethernet	Торгова
4.	65	10	9	2	7	1	Зірка	Fast Ethernet	Інформаційна
5.	10	7	7	2	9	1	Шина	FDDI	Електронна комерція
6.	28	5	1	2	1	1	Кільце	FDDI	Захист
7.	79	10	5	1	10	2	Шина	Fast Ethernet	Пошукова служба
8.	30	2	2	1	2	2	Зірка	Gigabit Ethernet	Поштова служба
9.	15	3	9	1	8	2	Кільце	FDDI	Послуги зв'язку
10.	24	8	6	2	7	1	Зірка	Fast Ethernet	Управління проектами
11.	73	10	1	2	11	1	Шина	Gigabit Ethernet	Навчальна
12.	32	11	8	2	5	1	Кільце	Fast Ethernet	Банківська
13.	65	5	11	1	9	2	Шина	Gigabit Ethernet	Торгова
14.	85	7	13	1	7	2	Зірка	Gigabit Ethernet	Інформаційна
15.	15	3	2	1	8	2	Кільце	FDDI	Електронна комерція
16.	95	13	14	2	1	1	Зірка	Fast Ethernet	Захист
17.	46	9	18	2	3	1	Шина	Gigabit Ethernet	Пошукова служба
18.	35	2	1	2	4	1	Кільце	Fast Ethernet	Поштова служба
19.	36	7	8	1	13	2	Шина	Fast Ethernet	Послуги зв'язку
20.	89	3	13	1	4	2	Зірка	Gigabit Ethernet	Управління проектами
21.	37	1	8	1	8	2	Кільце	Fast Ethernet	Навчальна
22.	81	45	15	2	2	1	Зірка	Fast Ethernet	Банківська
23.	94	6	9	2	20	1	Шина	Gigabit Ethernet	Торгова
24.	46	11	6	2	5	1	Кільце	Fast Ethernet	Інформаційна
25.	25	3	6	1	8	2	Шина	FDDI	Електронна комерція
26.	37	6	18	1	6	2	Зірка	Fast Ethernet	Захист
27.	15	1	3	1	4	2	Кільце	FDDI	Пошукова служба
28.	68	18	7	2	7	1	Зірка	Fast Ethernet	Поштова служба
29.	20	3	6	2	15	1	Шина	FDDI	Послуги зв'язку
30.	80	8	14	2	8	1	Кільце	Gigabit Ethernet	Управління проектами

Завдання для лабораторних робіт

Створення облікових записів користувачів та груп у Windows 2000

Завдання

1. Зареєструватись на консолі сервера з використанням облікового запису з адміністративними правами.
2. Створити локальні і глобальні групи відповідно до таблиці 1. Увести глобальні групи до складу локальних відповідно до таблиці 1 та надати привілеї локальним групам відповідно Таблиці 1 та таблиці 2.

Для створення і оперування з групами використовується оснащення: *Administrative Tools/Users and Computers*

Для призначення привілей використовується оснащення: *Administrative Tools/Local Security Policy/User Rights Assignment*

Таблиця 1

Назва групи	Тип	Членство	Привілеї
Local1	локальна		1, 3, 7, 10
Local2	локальна		2, 4, 3, 6
Local3	локальна		3, 11, 7, 10
Local4	локальна		1, 4, 6, 8
Global1	глобальна	Local1, Local2	
Global2	глобальна	Local3, Local4	
Global3	глобальна	Local1, Local3	
Global4	глобальна	Local2, Local4	

Таблиця 2

№	Привілеї	Описание
1	*Backup files and directories*	Виконувати резервне копіювання файлів та каталогів (пріоритет над правами доступу до файлів та каталогів)
2	*Load and unload device drivers*	Встановлювати та видаляти драйвери пристроїв
3	*Shutdown the system remotely*	Виконувати вимкнення віддаленої системи
4	*Restore files and directories*	Відновлювати файли та каталоги з резервної копії
5	*Manage auditing and security log*	Вказувати, які типи доступу до ресурсів підлягають реєстрування, а також дивитись та очищувати журнал аудиту
6	*Shutdown the system*	Вимикати систему
7	*Change the system time*	Встановлювати внутрішній таймер комп'ютера
8	*Take ownership on files or other objects*	Приймати файли, каталоги, принтери та інші об'єкти у власність
9	*Log on locally*	Реєструватися локально з клавіатури комп'ютера
10	*Access this computer from the network*	Підключатись до комп'ютеру по мережі

3. Створити власний обліковий запис та увести його у групу Domain Admins.

4. Зареєструватись за допомогою власного облікового запису.
5. Створити облікові записи відповідно до Таблиці 3.
6. Спробувати зареєструватись з консолі сервера за допомогою створених облікових записів. В тому випадку, коли система забороняє це зробити, пояснити причину та відкоригувати обліковий запис таким чином, щоб процес реєстрації відбувся.
7. На іншому комп'ютері завантажити Windows 2000 Professional. Спробувати зареєструватись на сервері (в домен Home). У випадку невдачі відкоригувати обліковий запис на сервері таким чином, щоб реєстрація була можливою.
8. Зробити висновки.

Таблиця 3

First name	Initials	Last Name	Logon name	Password	Group	Logon to	Hours
Ivan	A	Ivanov	IvanovI	ivan	Global1 Local2 Global4 Local3	Server WS17 WS14 WS11	Sunday 9:00–21:00 Saturday 13:00–17:00 Friday 2:00–11:00 Other 6:00–12:00
Peter	O	Petrov	PetrovP	petr	Global2, Local3 Global3 Local1	Server WS12 WS13 WS15	Sunday 3:00–11:00 Saturday 23:00–24:00 Friday 12:00–17:00 Other 2:00–18:00
Dmitriy	L	Sidorov	SidorovD	sidor	Global2 Local3 Global4 Local4	Server WS12 WS13 WS15	Sunday 8:00–15:00 Saturday 12:00–18:00 Friday 15:00–17:00 Other 1:00–3:00

Налаштування робочого середовища користувачів ОС Windows 2000

1. Засвоєння принципів роботи з редактором системної політики.

1.1. Додати в меню Administrative Tools оснастку Local Computer Policy, скориставшись програмою mmc.

1.2. Запустити редактор системної політики: Administrative Tools/Local Computer Policy.

1.3. Вибрати User Configuration/Administrative Templates.

1.4. За вказівкою викладача заблокувати певні можливості інтерфейсу і перевірити, що заборона діє.

1.5. Повернути налаштовування інтерфейсу до попереднього стану.

2. Створення завантажувальних профілів користувачів.

2.1. Створити обліковий запис Test і додати його в групу Domain Admins.

2.2. Зареєструватись під цим обліковим записом.

2.3. Змінити налаштування робочого столу та за вказівкою викладача внести зміни в системну політику (аналогічно п.1.3).

2.4. Зареєструватись за допомогою власного облікового запису.

2.5. Створити на диску С віртуальної машини папку із власним прізвищем.

2.6. Через праву кнопку миші вибрати My Computer/Properties/User Profiles.

2.7. Вибрати профіль користувача Test і скопіювати його в папку, створену в п.2.5, перед копіюванням встановивши дозвіл на користування цим профілем всім користувачам через об'єкт Everyone.

2.8. Створити новий обліковий запис користувача з довільним ім'ям.

2.9. У властивостях облікового запису в закладці Profile вказати шлях до папки, створеної в п.2.5.

2.10. Зареєструватись за допомогою облікового запису, створеного в п.2.8. Перевірити, чи завантажився призначений профіль.

2.11. Віддати папку, створену в п.2.5 до загального користування з правами повного доступу для всіх користувачів.

2.12. У властивостях облікового запису в закладці Profile вказати шлях до папки, створеної в п.2.5 у вигляді \\Server\FolderName, де FolderName – відповідне ім'я папки.

2.13. Повторити п.2.10, реєструючись з робочої станції.

3. Ознайомлення з політикою керування обліковими записами.

3.1. Запустити Administrative Tools/Domain Security Policy/Account Policies.

3.2. За вказівкою викладача встановити обмеження на довжину пароля, періодичність його зміни, складність і т.д.

3.3. Перевірити встановленні обмеження шляхом створення нового облікового запису.

3.4. Встановити налаштування, що запобігатимуть підбиранню паролю.

3.5. Перевірити дієвість налаштувань шляхом повторення спроб реєстрації із невірним паролем.

4. Зробити висновки.

Засвоєння принципів роботи з файловою системою NTFS

1. На NTFS розділі створити папки з правами згідно з таблицею 1. В кожній із папок створити текстовий файл з іменами відповідно File1.txt, File2.txt, File3.txt, File4.txt. Для надання прав необхідно натиснути праву кнопку миші на папці, на яку призначаються права, вибрати Properties/Security, додати відповідного користувача або групу та вибрати необхідні права.

2. Перевірити роботоздатність наданих прав. Для цього слід по черзі зареєструватись за допомогою облікового запису IvanovI, PetrovP, SidorovD та спробувати внести зміни до файлів, що знаходяться в каталогах Direct1,

Direct2, Direct3, Direct4. Пояснити результати.

Таблиця 1

Директорія	**Користувачі (групи)**	**Права**
Direct1	IvanovI Local1	Allow: Read, Write, List Folder Contents Deny: Read,Write
Direct2	Local2 PetrovP	Allow List Folder Contents, Read Allow Full Control
Direct3	SidorovD Local3	Allow: Read, Write Deny: Full Control
Direct4	Local4 PetrovP	Allow Write Deny: List Folder Contents, Read

3. Організувати аудит таких подій за вказівкою викладача:
   - невдалі спроби реєстрації;
   - вдалі і невдалі спроби створення користувачів;
   - перегляд вмісту папки Direct1 користувачем PetrovP;
   - спроба створення файлу користувачем IvanovI в папці Direct2.

Для активізації аудиту необхідно запустити Programs/Administrative Tools/Domain Controller Security Policy, вибрати Local Policies/Audit Policy. Активізувати аудит таких подій, як: реєстрація користувачів, доступ до об'єктів, операції з обліковими записами. Для активізації аудиту доступу до окремої папки окремим користувачем необхідно натиснути праву кнопку миші на папці, на яку призначається аудит, вибрати Properties/Security/Advanced. Далі вибрати закладку Auditing та за допомогою кнопки Add додати користувача або групу, чий доступ аудіюється. Далі вибрати типи операцій, які підлягають аудиту.

4. Ініціювати одну з подій, що підлягають аудиту.

5. Знайти відповідний запис в журналі захисту та зробити висновки. Результати аудиту можна переглянути, запустивши:
Programs/Administrative Tools/Event Viewer/Security Log.

6. Для перевірки функціонування Encrypted File System необхідно зареєструватись за допомогою облікового запису IvanovI, створити текстовий файл з ім'ям TestFile та записати в нього довільний текст. Надати на цей файл права доступу користувачу PetrovP. Натиснути праву кнопку миші на папці, на яку призначаються права, вибрати Properties/General, натиснути кнопку Advanced. Встановити атрибут «Encrypt contents to secure data». Далі зареєструватись за допомогою облікового запису PetrovP і спробувати переглянути вміст файлу. Зробити висновки. Зареєструватись за допомогою облікового запису, що входить до групи Administrators і також спробувати переглянути вміст файлу.

7. Зробити висновки.

Література

1. Зелинский С. Э. Microsoft Windows XP. – М.: Издательство Юниор, 2003. – 528 с.
2. Зозуля Ю. Н. Windows XP на 100%. – СПб.: Издательство “Питер”, 2007. – 528 с.
3. Курячий Г. В., Маслинский К. А. Операционная система Linux. Интернет-университет информационных технологий – www.intuit.ru.
4. Торчинский Ф. И. Операционная система Solaris. Интернет-университет информационных технологий – www.intuit.ru.
5. Курячий Г. В. Операционная система Unix. Интернет-университет информационных технологий – www.intuit.ru.
6. Костромин В. А. Linux для пользователя. – СПб.: БХВ–Петербург, 2002. – 672 с.
7. Петерсен Р. Энциклопедия Linux. – СПб.: Издательство “Питер”, 2002. – 1008 с.
8. Колисниченко Д. Н. Linux-сервер своими руками. – М.: Наука и Техника, 2002. – 576 с.
9. К. Закер Компьютерные сети. Модернизация, поиск неисправностей. – СПб.: БХВ–Петербург, 2002. – 1008 с.
10. Буров Є. Комп’ютерні мережі. – Львів: БаК, 1999. – 468 с.
11. Кульгин М. Технологии корпоративных сетей. Энциклопедия – СПб.: Издательство “Питер”, 2000. – 704 с.
12. Олифер В. Г., Олифер Н. А. Компьютерные сети: принципы, технологии, протоколы. – СПб.: Издательство “Питер”, 2001. – 672 с.
13. Э. Таненбаум Компьютерные сети. – СПб.: Издательство “Питер”, 2002 – 848 с.

Навчальне видання

Сергій Михайлович Захарченко
Олена Іванівна Суприган

ОСНОВИ СИСТЕМНОГО АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ НА БАЗІ ОС WINDOWS

Навчальний посібник

Оригінал-макет підготовлено Суприган О. І.

Редактор Старічек Т. О.

Науково – методичний відділ ВНТУ
Свідоцтво Держкомінформу України
серія ДК № 746 від 25.12.2001
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ

Підписано до друку
Формат 29,7×42 1/4
Друк різографічний
Тираж _____ прим.
Зам. №

Гарнітура Times New Roman
Папір офсетний
Ум. друк. арк

Віддруковано в комп'ютерному інформаційно-видавничому центрі
Вінницького національного технічного університету
Свідоцтво Держкомінформу України
Серія ДК № 746 від 25.12.2001
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ