**Операційна система MS Windows.**

**Порівняння з іншими ОС**

**(Unix, Apple, Linux, BeOS та ін.)**

***Огляд існуючих ОС***

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***ОС*** | ***Платформа*** | ***Архітек-тура***  ***(bit)*** | ***Ядро*** | ***RAM***  ***(Мв)*** | ***Об’єм жорстк диску***  ***(Мв))*** | ***Власна файл. сист.*** | ***Сторонні файл. сист.*** | ***Переваги*** | ***Недоліки*** |
| *MacOS* | Power PC | 32 | монолітне | ≥8 | ≥120 | HFS, HFS+ | FAT, FAT32, ISO9660, UDF | Платформа для настільних видав-ничих систем, гра-фічнрго дизайну, Web-дизайну, офіс-них прикладних програм | Не вигідна для сервених прикладних програм та ігор |
| *Linux* | Intel, Power PC, Alpha, Motorola 68K, SPARC, UltraSPARC, ARM, MIPS | 32, 64 на Alpha I Ultra SPARC | монолітне | 8 | 200-600 | Ext2 | FAT, FAT32, ISO9660, UDF, HFS, SYSV, HPFS, NTFS, Minix | Гнучка основа для Internet-клієнтів, Internet-, Intranet- і файлових серверів, серверів баз даних, а також для зви-чайних офісних робіт | Невелика кількість сучасних ігор і відсутність побутових прикладних програм |
| *FreeBSD* | Intel, експериментально Alpa | 32 (Intel), 64 (Ultra SPARC) | монолітне | 8 | 150-350 | UFS | FAT, ISO9660, NTFS | стабільна і без-платна система для баз даних, Internet-, Intranet- і файлових серверів | Мало офісного програмного забезпечення, дуже мало ігор |
| *Solaris* | Intel, SPARC, UltraSPARC | 32 (intel), 64 (Ultra SPARC) | монолітне | Мінімум 32 | Від 500 | UFS | FAT, FAT32, ISO9660 | стабільна система для баз даних, In-ternet-, Intranet- і файлових серверів, Internet-Client, Java-розробок | Мало офісного програмного забезпечення, дуже мало ігор |
| *SCO Unix* | Intel | 32 (Intel), 64 (на стадії розроб ки) | монолітне | 32 | 0,5-1 Гб | VxFS, BFW | SS, UFS, SFS, FAT, ISO9660 |
| *OS/2 Warp Server* | Intel | 32 | монолітне | ≥32 | ≥350 | HPFS, JFS | FAT, FAT32, VFAT, NTFS, ext2fs, HFS | Стабільна система для підприємниць-ких мереж, кому-нікацій і серверів транзакцій, об’єд-нує різні платфор-ми | Недостатньо програмного забезпечення для приватних користувачів |
| *BeOS* | Intel, Power PC | 32 | MACH | ≥16 | ≥150 | JFS | FAT, FAT32 | Оптимальна для мультимедійних прикладних програм (відео-монтаж і звукова обробка) та ігор | Для офіснрго використання відсутнє відповідне ПЗ |
| *JavaOS* | Pentium | Від 32 до 128 | мікроядро | 32 | Дистанційно від NT-сервера |  |  | Не залежить від платформи сере-довища підтримки розробки | Відсутність стандартних застосувань |
| *Windows CE* | SH3, MIPS 39xx I 4xx, 486, Pentium, Power PC, Motorola, ARM/StrongARM | 32 | монолітне | 32 | 1 ROM- 2.5 |  |  | система з малим використанням енергії для мобіль-них Handheld-ПК і палитопів | Відсутність мультимедійних прикладних про-грам і трудоєм-ких застосувань |

***Windows 97***

1. Загальні відомості

Операцiйна система Windows-97 (надалi - W97) має значно розвинутiші мережнi функцiї порiвняно з її попередницями. Розробники її намагалися створити у функцiональному планi найсучаснішу мережну ОС, яка б задовiльняла основним вимогам до сучасних ОС:

1. простота в керуванні та можливiсть роботи малоквалiфiкованого користувача;
2. унiверсальнiсть; пiдтримка максимальної кiлькостi протоколiв та взаємодiя з багатьма мережними ОС;
3. поєднання зручностi та простоти адмiнiстрування з розвинутими адмiнфункцiями та можливiстю адмiнiстрування мереж з тисяч комп’ютерiв (зменшення витрат на адмiнiстрування);
4. вбудованiсть в систему електронної пошти та iнших засобiв колективної роботи i вихiд в глобальнi мережi;
5. пiдтримка вiддаленого доступу, мобiльних користувачiв.

W97 - це однорангова ОС з можливiстю пiдключення до серверiв Windows NT та Novell Netware. Що ж нового принесла W97 у свiт комп’ютерних мереж?

1. У системнiй архiтектурi - багатомодульна архiтектура, що налагоджується на пiдтримку рiзноманiтних функцiй за бажанням користувача вiдповiдним набором модулiв. Пiдтримка багатопротокольностi.
2. У засобах керування системними параметрами. Збереження системної iнформацiї в єдинiй базi даних - системному реєстрi. Подiл цiєї бази на користувацьку та машинну компоненти, що дозволяє однаково обслуговувати користувача незалежно вiд мiсця його входу у мережу. Простi та наочнi засоби роботи з реєстром.
3. У засобах iнсталяцiї. Можливiсть автоматизацiї процесу iнсталяцiї, створення спецiальних сценарiїв iнсталяцiї. Встановлення великої кiлькостi копiй ОС без втручання оператора. Налагодження функцiональностi системи на окремих користувачiв та їх групи.
4. У засобах взаємодiї з iншими системами. Крiм пiдтримки одноранговостi, можливiсть бути клiєнтом для систем Windows NT та Novell Netware. Можливiсть бути сервером для клiєнтiв Windows NT та Novell Netware. Додаткове пiдключення до iнших серверiв. Унiфiкацiя механiзму таких пiдключень.
5. У засобах адмiнiстрування. Можливiсть налагодження робочого середовища для рiзних користувачiв та їх груп (профiлi користувачiв). Пiдтримка iндивiдуального списку паролiв доступу до рiзних ресурсiв. Користувач вводить пароль лише один раз - при входi у систему. Користувач може входити в мережу на рiзних комп’ютерах i користуватися одними профiлями (робоче середовище слiдує за користувачем при його перемiщеннi). Можливiсть створення обов’язкових профiлiв. Використання системних правил для окремих користувачiв та їх груп для обмеження свободи змiн системних параметрiв на робочих мiсцях.
6. У системi електронної пошти. Система електронної пошти iнтегрована в ОС. Це означає, що iснує єдиний клiєнт електронної пошти, який обслуговує як локальну пошту, так i вихiд у зовнiшнi мережi. Вiн пiдтримує додатковi спорiдненi служби (наприклад, передавання факсiв). Така iнтегрованiсть електронної пошти дозволяє використовувати її прямо з застосувань.
7. У пiдтримцi вiддаленого доступу. Реалiзацiя основних протоколiв вiддаленого доступу. Наявнiсть утiлiт синхронiзацiї каталогiв.

Поряд з досягненнями, W97 має i ряд недолiкiв. Зокрема пiдтримується тiльки застарiла версiя Novell Netware (без можливостi роботи з деревом каталогiв). Є недолiки в механiзмi захисту системи, в доменнiй архiтектурi мереж Windows NT та iн.

Для зручностi користувача ОС та структурування мережних функцiй у W97 видiленi наступнi типи мережних компонент.

1. **Мережний адаптер**. Ця компонента містить як параметри реального мережного адаптеру, так i протоколiв PPP, SLIP. Одночасно може бути сконфiгуровано кiлька адаптерiв.
2. **Протокол.** Як правило - це визначення певних протокольних стекiв (IPX/SPX, Microsoft DLC, NetBEUI, TCP/IP). Протоколи ‘прикрiплюються’ до адаптерiв та мережних клiєнтiв. Одночасно може пiдтримуватись кiлька протокольних стекiв.
3. **Клiєнт.** Мережний клiєнт дозволяє з’єднуватися з серверами вiдповiдних мереж. Допускається встановлення клiєнтiв Banyan, FTP Software, Microsoft, Novell, Sunsoft. Клiєнти Microsoft, Novell не вимагають додаткового ПЗ.
4. **Служба**. Мережна служба - це сукупнiсть засобiв, якi виконують певну мережну функцiю. Наприклад, ‘Служба доступу до файлiв та принтерiв’. Окремо визначенi такi служби для мереж Microsoft та Novell.

**2. Iнсталяцiя та налагодження мережних компонент.**

Iнсталяцiя мережних компонент може вiдбуватися як пiд час iнсталяцiї самої ОС, так i пiд час роботи системи. Розробники ОС спробували максимально спростити процес iнсталяцiї на окремiй станцiї, приховати деякi його складнi нюанси, зрештою автоматизувати процес iнсталяцiї рiзних конфiгурацiй системи на велику кiлькiсть комп’ютерiв. У цьому розділі ми будемо звертати більшу увагу на основнi принципи та пiдходи, технiчнi та системнi рiшення, застосованi у процедурах iнсталяцiї мережних компонент W97, а не на детальну послiдовнiсть дiй користувача при цьому.

Перед iнсталюванням W97 треба вибрати мiсце розмiщення системи (локальний ПК або сервер), мiсце, з якого проводити iнсталяцiю (локальний ПК або сервер), а також варiант початкового завантаження системи (з жорского диску локального ПК, з сервера, з гнучких дискiв).

У залежностi вiд мiсця розмiщення системи розрiзняють наступнi конфiгурацiї.

1. Локальну - всi файли W97 розташованi на клiєнтi, iнсталяцiя проводиться з локальних дисководiв або з сервера. Така конфiгурацiя збiльшує швидокодiю роботи системи, але вимагає значного дискового простору.
2. Сумiсного використання - частина файлiв на клiєнтi, основна - на серверi. Встановлення системи вiдбувається з сервера. Це дозволяє зекономити ресурси, але призводить до зменшення швидкодiї роботи W97 в порiвняннi з локальною iнсталяцiєю.

У залежностi вiд мiсця, з якого iнсталюється система можливi такi варiанти.

1. Інсталяцiя з локального дисководу. При iнсталяцiї з локального дисководу дистрибутив міститься на локальному комп’ютерi. Система розмiщується на визначеному каталогу локального РС (локальна iнсталяцiя). Використовується для iнсталяцiї окремих, необ’єднаних iснуючою попередньо мережею станцiй. Дає менше можливостей для автоматизацiї процесу iнсталяцiї.
2. Інсталяцiя з сервера. Дистрибутив розміщується на серверi. Для такого типу iнсталяцiї необхiдне попереднє пiд’єднання до сервера у вже iснуючий мережi. Допускається як локальна інтсталяція, так i iнсталяцiя сумiсного використання. З сервера можна проводити iнсталяцiю на багато станцiй одночасно, застосувати засоби автоматизованої iнсталяцiї. При iнсталяцiї з сервера дистрибутив попередньо копiюється на диск сервера (команда **netsetup**).

Розглянемо детальнiше процес iнсталяцiї з точки зору засобiв його автоматизацiї.

**Першим** таким засобом слiд вважати можливiсть **автоматичного розпiзнавання типу адаптерної плати та встановлення необхiдних параметрiв** (технологiя plug and play). Встановленi параметри плати (номер переривання, адресу вводу-виводу можна пiзнiше проставити i вручну. При цьому система буде вiдмiчати можливi конфлiкти i пiдказувати дiапазони можливих значень.

**Другим** таким засобом є **встановлення мережних компонент ‘за замовчуванням’.** У процесi iнсталяцiї користувач задає необхiднiсть використання рiзноманiтних мережних компонент. *При виборi однієї компоненти автоматично встановлюються i iншi, залежнi вiд неї компоненти у стандартних конфiгурацiях*. При цьому користувач пiзнiше зможе не тiльки переглянути встановлену конфiгурацiю, але й модифiкувати згiдно зі своїми потребами. Наприклад, якщо виявлено мережний адаптер, автоматично встановлюються наступнi компоненти.

1. Клiєнт для мереж Microsoft

дозволяє комп’ютеру стати клiєнтом мереж SMB (Service Message Block - протокол передавання файлiв) - мереж WNT, W for WKG, LAN Manager, OS/2 LAN Server.

1. Клiєнт для мереж Netware

дозволяє комп’ютеру стати клiєнтом до мереж Netware 2.15 - 3.х. Версiя 4.х пiдтримується тiльки в режимi емуляцiї bindery.

1. IPX/SPX сумiсний протокол.
2. NETBEUI.

**Третiм** засобом автоматизацiї iнсталяцiї слiд вважати можливiсть створення та **використання текстових командних файлiв** керування iнсталяцiєю. Назву командного файлу (з розширенням **inf**) можна вказати в командному рядку:

**setup myfile.inf**

Якщо назва файлу не вказана, використовується системний файл **msbatch.inf**. Командний файл має власний формат. Якi ж параметри можна занести в цей файл? Перш за все це параметри, що заносяться користувачем вручну при iнсталяцiї, параметри вибору та налагодження протоколiв та iнших мережних компонент, список додаткових програм яких треба проiнсталювати (в тому числi i тих, що не входять у склад дистрибутива W97 - використання утiлiти **infinst**.) У командних файлах адмiнiстратор може активiзувати користувацькi профiлi та ввімкнути пiдтримку системних правил.

Використання командного файлу дозволяє повнiстю автоматизувати процес iнсталяцiї i проводити його одночасно на велику кiлькiсть комп’ютерiв без участi оператора. Для формування командного файлу можна використати **ХХХХХХХХХ**

Це компактна утiлiта, яка дозволяє створити до 9999 пакетних файлiв iнсталяцiї (тобто за один раз iнсталювати 10000 комп’ютерiв). Цi файли розмiщуються у видiленому каталозi (BSTP00001.INF - BSTP9999.INF). Файли узагальнюються у ведучому текстовому файлi, що складається з рядкiв

**Iм’я РС [, адреса IP]**

кожний рядок вiдповiдає комп’ютеру, на якому проводиться встановлення. Утiлiта також дозволяє вiдкривати наявні скрипти та модифiкувати їх. У процесi роботи утiліти задаються всi основнi параметри інсталяцiї. Наприклад, можна примусити зберiгати ininstall-iнформацiю, встановлювати набiр необов’язкових компонент.

Автоматичну iнсталяцiю можна проводити наступними шляхами:

1. використати пакетний DOS-файл з командами встановлення мережного з’єднання та запуску iнсталятора;
2. використати макрос вiдкриття сеансу при входi у мережу;
3. використати групу автозапуску;
4. можна вiдправити об’єкт електронної пошти, при виборi якого користувачем автоматично запуститься iнсталятор;
5. використати програмне забезпечення керування мережею, програми дистанцiйного керування.

**3. Робота в мережi.**

3.1. Мережнi компоненти та їх налагодження.

За своєю структурою та iнтерфейсом взаємодiї з оператором W97 є об’єктно- орiєнтованою ОС. З цього випливає подання системи як набору компонент зi своїми властивостями. Однi i тi ж операцiї у W97, як правило, можна провести кiлькома рiзними шляхами.

Пiсля встановлення системи користувач має деяку мережну конфiгурацiю, параметри якої були визначенi пiд час iнсталяцiї. Але й пiд час роботи системи користувач має можливiсть аналiзувати мережну конфiгурацiю, iнсталювати або деiнсталювати її окремi компоненти.

Розглянемо бiльш детально окремi мережнi компоненти.

Адаптери

W97 безпосередньо взаємодiє з вiдповiдним драйвером адаптера. W97 пiдтримує драйвери в форматах NDIS 3.1 (32-розр), NDIS 2.x(16-розр) та ODI. Драйвер формату NDIS 3.0, що був у Windows for Workgroups (WKG), не пiдтримується.

Протоколи

Загальною рисою форматiв драйверiв NDIS та ODI є забезпечення багатопротокольного стеку. Кiлька протоколiв використовують для передавання один i той же адаптер. Кажуть, що протоколи закрiпленi за адаптером (прив’язанi, bind). У W97 протоколи реалiзованi як 32-розряднi драйвери захищеного режиму VXD (Virtual Device Drivers). Пiдтримуються такi протоколи:

1. NETBEUI - NetBIOS Extended User Interface - протокол сумiсний з стандартним протоколом NETBEUI, який використовується у WKG, WNT, OS/2, LAN Server. Цей протокол розроблено IBM. Вiн не пiдтримує передавання маршрутної iнформацiї. Але вiн може працювати з мостами.
2. IPX/SPX.
3. TCP/IP.

Клiєнти. Клiєнтний компонент дозволяє комп’ютеру мати доступ до серверiв вiдповiдних мереж. Для кожного типу мережi встановлюється окрема клiєнтна компонента.

Клiєнти бувають 32-розрядного захищеного режиму та 16-розрядного реального режиму. Можна встановити один клiєнт реального режиму та довiльну кiлькiсть клiєнтiв захищеного режиму. У поставку входять клiєнти мереж Microsoft, Novell, FTP, Sunsoft, Banyan.

Клiєнт для мереж Microsoft дозволяє працювати з усiма SMB (Server Message Block)-сумiсними мережами. Клiєнт для мереж Novell дозволяє працювати з усiма NCP (Netware Core Protocol)-мережами. На сьогоднi клiєнт не пiдтримує NDS Novell 4.1, а працює з ним тiльки в режимi емуляцiї bindery.

Протоколи SMB та NCP - це протоколи сумiсного використання файлiв. Вони регулюють розподiл файлiв мiж робочими станцiями. Цi протоколи не обираються iндивiдуально, а вбудованi в клiєнтнi та сервiснi компоненти ОС.

У W97 один протокол може бути прив’язаний до кiлькох клiєнтiв або кiлька протоколiв до одного клiєнта. Наприклад,

NETBEUI

Клiєнт Microsoft

IPX/SPX

Клiєнт Novell

Рис. 1. Прив’язування протоколів до клієнтів.

Але при реалiзацiї взаємодiї сервер та клiєнт користуються одним протоколом.

Служби

Мережна служба - це сукупнiсть засобiв, якi дозволяють вирiшувати конкретну сервiсну функцiю (сумiсне використання принтерiв та файлiв, пiдтримка створення мережних резервних копiй та iн.). У W97 є двi служби, що дозволяють клiєнтам iнших мереж мати доступ до файлових та принтерних ресурсiв локального комп’ютера:

**File and Printer Sharing for Microsoft Networks**

**File and Printer Sharing for Netware Networks**

Цi служби встановлюються за замовчуванням.

3.2. Реєстрацiя користувача у системi.

Розглянемо процес входження користувача у систему. У W97 можна задати один з трьох варiантiв входження.

1. Клiєнт для мереж Microsoft. Встановлюється за замовчуванням.
2. Клiєнт для мереж Netware.
3. Звичайне входженння у Windows - не дiє механiзм захисту щодо користувачiв- якщо пiд час першого запуску не вказувати пароль, то вiкно iдентифiкацiї користувача не буде з’являтися. Iм’я та пароль запитують тiльки у випадку активiзацiї користувацьких профiлiв.

Якщо встановлено пiдключення до мережi Microsoft, введене iм’я та пароль перевiряються на серверi WNT.

Аналогiчно, якщо входимо з пiд’єднанням до Netware, W97 запам’ятовує паролi у списку паролів i не питає їх при наступнiй спробi увiйти у мережу. Якщо пароль входження у W97 зробити пустим i увiйти в сервер WNT або Netware, то при наступнiй спробi увiйти в систему пароль не буде запитуватися, i користувач отримає пiдключення до сервера без перевiрки.

Якщо ваші iм’я та пароль входження у W97 спiвпадають з iменем та паролем входження у WNT або Netware, то цi данi служать перепусткою на вiдповiдний сервер. Якщо ж iм’я та пароль невiдомi серверу, то при пiд’єднанні до нього необхiдно ввести iм’я та пароль, якi будуть збереженi у списку паролiв користувача. У наступний раз пароль буде зчитуватись зі списку.

3.3. Використання засобу ‘Network Neighborhood` (NN).

Значну кiлькiсть операцiй можна виконати засобами NN. Наприклад, переглядати спiльнi ресурси на серверах мережi або вiдображати ресурс на мережний диск. При цьому первинним форматом вiдображення ресурсу є **UNC (Universal Naming Convention)**-нотацiя. **\\iм’я комп’ютера\ресурс**

У мережi W97 кожний комп’ютер має унiкальне iм’я, що визначається при iнсталяцiї системи. Ресурс може зображати диск комп’ютера, каталог або принтер. Використання UNC-формату мережних ресурсiв дозволяє обiйти обмеження на кiлькiсть мережних ресурсiв. Вiдображення ресурсу на його позначення (наприклад D:, G:, або LPT1) називається перехопленням.

При переглядi мережних ресурсiв система використовує паролi зi списку паролів або запитує пароль.

Пiд’єднання до мережних принтерiв. Перед пiд’єднанням необхiдно встановити драйвер принтеру. Це можна зробити з iнсталяцiйного диску або з наявного мережного принтера. При встановленнi принтера у W97 - ресурс можна задавати в UNC-нотацiї. Застосування DOS не розумiють UNC-формату i треба реалiзовувати перехоплення принтера. Перехоплення реалiзується автоматично при виборi опцiї роботи з DOS при встановленнi принтера або через пункт меню ‘Призначити порт’.

Перегляд та пiд’єднання/вiд’єднання мережних дискiв можна також проводити засобами програми explorer.

3.4. Робота з командним рядком.

Командний рядок W97 дозволяє вводити глобальнi для всiєї системи команди, запускати windows-програми, а також цiлi команднi файли. Деякi команди:

|  |  |
| --- | --- |
| NET CONFIG | Вiдображення бiжучої конфiгурацiї РС. |
| NET DIAG | Запускає програму дiагностування мережi. Перший РС с запущеною командою буде дiагностичним сервером. Вiн буде присилати за запитом iнших станцiй дiагностичну iнформацiю. |
| NET HELP | Допомога. |
| NET PASSWORD | Змiна пароля для вiдкриття сеансу на конкретному серверi або доменi. |
| NET PRINT | Вiдображення iнформацiї про чергу на друк i керування завданнями на друк. |
| NET TIME | Синхронiзацiя часу на локальному РС з годинником сервера. |
| NET USE | Вiдображає наявні з’єднання з мережними дисками та принтерами. Встановлює та припиняє такi з’єднання. |
| NET VER | Вiдображення номера версiї програми. |
| NET VIEW | Список серверiв групи та їх ресурсiв. |

Якщо iм’я комп’ютера мiстить пробiл, то команда NET з ним не працює.

Формат NET USE:

**NET USE [пристрій:] \\комп’ютер\ресурс [пароль | ? ] [/SAVEPW:NO] [/YES] [/NO]**

SAVEPW:NO означає, що пароль не треба запам’ятовувати у списку паролiв. [/YES] [/NO] - вказання варiантiв автоматичних вiдповiдів на всi питання. Для вiд’єднання використовується ключ /D.

**4. Керування мережею.**

4.1. Iдентифiкацiя комп’ютера та механiзми обмеження доступу.

Пiд час iнсталяцiї вказується мережне iм’я та група, в яку входить комп’ютер. Цi параметри можна змiнити. Робоча група - це лише зручний засiб для групування комп’ютерiв.

У W97 визначено два механiзми керування доступом до ресурсiв. Керування доступом на рiвнi ресурсiв дозволяє призначати паролi довiльному ресурсу. Керування на рiвнi користувачiв дозволяє вказати конкретних користувачiв або їх групи, що мають доступ до кожного ресурсу. Керування доступом на рiвнi користувачiв допускається тiлькi при пiд’єднанні до серверiв Netware або WNT. При цьому вiдповiднi права зчитуються з цих серверiв. Якщо доступ дiє на рiвнi ресурсiв, W97 дозволяє задати повний доступ або доступ для читання. Якщо доступ дiє на рiвнi користувачiв, крiм повного доступу та доступу за читанням, можна ще задати права на:

1. читання файлiв;
2. запис файлiв;
3. створення файлiв та папок;
4. знищення файлiв;
5. змiна атрибутiв файлу;
6. роздрук файлу;
7. змiна керування доступом.

Незважаючи на те, що Netware та WNT дозволяють призначати права доступу до окремих файлiв та каталогiв, W97 дозволяє призначати права тiльки для каталогiв. За замовчуванням дiє керування доступом на рiвнi ресурсiв. Вибiр типу сервера отримання iнформацiї про права доступу користувачiв визначається встановленою службою (Microsoft або Netware).

4.2. Спiльне використання файлiв та принтерiв.

Комп’ютер можна сконфiгурувати, як файловий сервер або сервер друку. За замовчуванням сумiсне використання не встановлено. Пiсля його встановлення зробити каталог сумiсним можна в Explorer. Вказується мережне iм’я ресурсу. Якщо треба зробити, щоб iншi користувачi не могли переглядати iм’я даного ресурсу, в кiнець iменi додається $ наприклад, **public$.**  Задається тип доступу: тiльки для читання, повний, визначений паролем. У останньому випадку тип доступу буде визначатися введеним паролем.

Якщо визначений доступ на рiвнi користувачiв, також задається iм’я ресурсу. Крiм того, виводиться список користувачiв та груп, що мають право доступу до ресурсу. При додаванні нових користувачiв можна задати тип доступу (читання, повний або спецiальний). Режим ‘спецiальний’ дозволяє задати права доступу.

Сумiсне використання принтерiв керується аналогiчно до сумісного викоримтання файлів.

4.3. Реєстр W97 та керування мережними параметрами.

Основними об’єктами керування є ‘системний реєстр’, ‘користувацькi профiлi’, ‘системнi правила’. Кожний користувач може мати власнi налагодження (свiй профiль). У профiль входять конфiгурацiя робочого столу, змiст меню та iн. Користувач може мати доступ до свого профiлю з довiльного комп’ютера. Системний реєстр складається з двох файлiв: USER.DAT (користувацькi налагодження, незалежнi вiд комп’ютера, перемiщуються з користувачем на iншi ПК) та SYSTEM.DAT (системнi та апаратнi параметри залежнi вiд ПК, не перемiщуються). Системнi правила дозволяють адмiнiстратору встановлювати права для користувачiв та системнi параметри для РС.

Системний реєстр W97 - це iєрархiчна база даних для збереження системної iнформацiї. ini-файли використовуються частково для застосувань, якi не взаємодiють з реєстром. За замовчуванням системнi файли містяться в каталозi \Windows\System, але можуть бути i в iнших каталогах.

Програма роботи з реєстром - **regedit**. Основнi папки реєстру:

1. HKEY\_LOCAL\_MACHINE
2. HKEY\_USERS

вiдповiдають файлам реєстру. Iншi папки є окремими гiлками цих двох папок:

HKEY\_CURRENT\_CONFIG вiдповiдає роздiлу config HKEY\_LOCAL\_MACHINE

1. HKEY\_DYN\_DATA вказує на областi, що мiстять iнформацiю про пристрої plug and play.
2. HKEY\_CLASSES\_ROOT - це роздiл HKEY\_LOCAL\_MACHINE\Software\Classes для асоцiювання файлiв з застосуваннями.
3. HKEY\_CURRENT\_USER - це роздiл HKEY\_USERS, що мiстить iнформацiю про профiль користувача, який використовує ПК в даний момент.

Окремi роздiли HKEY\_LOCAL\_MACHINE.

1. Config - рiзнi апаратнi конфiгурацiї, можливi для даного комп’ютера.
2. Enum - iнформацiя про пристрої даного комп’ютера . Монiтори, НЖМД, НГМД, мережнi протоколи та iн.
3. Network - iнформація про конфiгурацiю мережi.
4. Security - iнформація про безпеку та дистанцiйне адмiнiстрування.
5. Software - програмне забезпечення, встановлене на комп’ютерi.
6. System - iнформація про встановленi драйвери, служби, назву комп’ютера, параметри файлової системи та iн.

Окремi роздiли HKEY\_USERS.

1. Сontrol Panel - користувацькі встановлення панелi керування.
2. InstallLocationMRU - список шляхiв iнсталяцiї W97 та iнших продуктiв.
3. Network - список популярних мережних з’єднань.
4. RunMRU - список застосувань, що використовуються популярними мережними з’єднаннями.
5. RemoteAccess - параметри вiддаленого доступу.
6. Software - програмнi встановлення користувача для застосувань.
7. StreamMRU - документи, що використовувалися останнiм часом.

**Операцiї з системним реєстром.**

Iмпортування та експортування даних з реєстру.

Можна iмпортувати окрему гiлку реєстра (з усiма вкладеними) або весь реєстр. Експортований файл має текстовий формат i може змiнюватись текстовим редактором. Експорт та iмпорт можна проводити i з командного рядка.

Iмпорт:

**REGEDIT [/L:system] [/R:user] filename.reg**

розмiщення системних файлiв

назва файлу, що iмпортується

Якщо iмпортується частина файлу, то вона замiняє вiдповiднi роздiли реєстру.

Експорт:

**REGEDIT [/L:system] [/R:user] /E filename.reg [regkey]**

параметр regkey задає початковий ключ реєстра, з якого вiдбувається експорт.

Якщо треба повнiстю замiнити реєстр, використовується ключ /С.

Користувацькi профiлi.

У користувацьких профiлях зберiгається iнформація про встановлення робочого столу, популярнi мережнi ресурси, з’єднання. Локальнi користувацькi профiлi зберігаються у папцi \Windows\Profiles. Для кожного користувача - окрема папка. У цiй папцi є наступнi папки:

1. Desctop - ярлики на робочому столi;
2. NetHood - iнформація про вiкно мережного оточення;
3. Recent - вмiст пункту ‘Документи’ головного меню;
4. Start Menu - змiст меню ‘Старт’;
5. USER.DAT - користувацька частина системного реєстру;
6. USER.DA0 - її копiя.

Розташування каталогу, який мiстить файл зi списком шляхiв знаходження користувацьких профiлів. Розташування каталогу користувацьких профiлів визначене пiд ключем

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\ProfileList

При входi користувача в систему введене ним iм’я служить основою для пошуку файлу користувацьких профiлів. Паролi містяться в каталозі \Windows. Файл паролiв Zak.pwl

Для того, щоб примусити використовувати профiлі з локальної машини, а не з сервера треба провести встановлення HKEY\_LOCAL\_MACHINE. Logon. Зробити новий параметр **UseHomeDirectory** типу DWORD. Такий параметр дiє для даного комп’ютера i для всiх користувачів, що працюють на ньому.

Якщо користувача немає, використовується профiль за замовчуванням.

Користувацькi профiлi в мережному середовищi можуть зберiгатись на серверi. При входi користувача порiвнюються профiлi на серверi та локальний. Вибирається найновiший. Пiсля цього оновлюється серверний профiль. Цей профiль оновлюється i при виходi користувача. Iнформацiя про профiлi може зберiгатись на серверi WNT, NETWARE, W97.

Загальнi умови для роботи з серверним збереженням користувацьких профiлів:

1. повинен бути встановлени вiдповiдний 32-розрядний клiєнт;
2. мережний сервер повинен пiдтримувати довгi iмена файлiв;
3. на всiх клiєнтах W97 повинна бути встановлена в каталозi з однаковою назвою.

Умови роботи з WNT.

Користувач має базовий каталог на серверi. Активiзованi профiлi. Опцiя входу - пiдключення до домена WNT (якщо вибрати швидкий вхiд, зчитування профiлів з сервера не вiдбудеться, активiзується локальний профiль i оновлення профiлів вiдбудеться за локальним профiлем (який може бути застарiлим).

***Робота з W97 - сервером.***

У HKEY\_LOCAL\_MACHINE\Network\Logon введено значення SharedProfileList та UseHomeDirectory. Перше значення вказує на файл зi списком профiлів. Наприклад, це може бути UNC - \*.ini файл з такими рядками:

**[Profiles]**

**Dana=\\zak\public\dana\user.dat**

**Katie=\\zak\public\katie\user.dat**

У ОС W97 можливе застосування обов’язкових користувацьких профiлiв. Це обов’язковi користувацькi профiлi, якi зберiгаються на серверi. Цi профiлi не можуть бути змiненi користувачем. Файл USER.DAT на серверi переiменовується на USER.MAN.

Системнi правила.

Системнi правила дозволяють гнучіше адмiнiструвати роботу окремих користувачiв та їх груп. Основні функцiї та положення:

1. системнi правила можуть використовуватись окремо для користувацької та системної частини реєстру;
2. можна використовувати iндивiдуальнi та груповi правила з перекриттям;
3. можливе використання обов’язкових профiлів та системних правил одночасно.

Умови використання системних правил:

1. для реалiзації користувацьких правил - активiзованi профiлi;
2. на серверi WNT або NETWARE зберiгається файл системних правил **CONFIG.POL**;
3. якщо використовується iнший сервер - мусять бути проведенi встановлення в реєстрi.

Для створення системних правил використовується редактор **POLEDIT.EXE**. Цей редактор комплектується файлом-шаблоном ADMIN.ADM, який вказує, якi параметри системного реєстру доступнi у редакторi. Файл-шаблон можна редагувати та додавати в нього новi параметри. Файл системних правил мiстить правила ‘Стандартний комп’ютер’ та ‘Стандартний користувач’.

Кожний елемент в редакторi можна відмiтити як реалiзований, нереалiзований, незмiнний. Першi два змiнюють вiдповiдний параметр у системному реєстрi. Реалiзований - встановлює, нереалiзований - скидає. Незмiнний - залишає встановлене користувачем значення.

**Схема застосування правил.**

Коли користувач вiдкриває сеанс, то, якщо для цього користувача iснують певнi правила, вони використовуються. Якщо користувач не має персональних правил, але входить у групи, застосовуються правила груп. Завантаження правил йде вiд найменшого пріоритету до найбiльшого. Якщо для користувача не iснує правил, застосовуються правила ‘Стандартний користувач’. Правила застосування комп’ютерних правил - аналогiчнi.

Окремо встановлюється редактор системних правил та групових правил \ADMIN\APPTOOLS\POLEDIT окремо, з диску. Груповi правила встановлюються на всiх ПК, де використовуються групи. Редактор системних правил працює в двох режимах - режимi файла правил (змiна файлу правил) та режимi реєстру (змiна параметрiв реєстру з використанням шаблонiв правил). При створеннi нового файла правил автоматично створюються об’єкти ‘Стандартний користувач’ та ‘Стандапртний комп’ютер’. Новi правила при створеннi iдентичнi стандартним, а потiм змiнюються вручну. Використовуючи редактор правил, можна модифiкувати правила на вiддаленому комп’ютерi.

Розмiщення config.pol:

WNT: \\server\_name\netlogon\

Netware: \\ server\_name\sys\public\

Встановлення.

Користувацькі:

1. панель керування:
2. екран, мережа, паролi, принтери, система;
3. робочий стiл:
4. фон, кольорова схема;
5. мережа:
6. доступ;
7. оболонка:
8. власнi папки, обмеження;
9. система:
10. обмеження.

Системнi:

1. мережа:
2. керування доступом, вхiд у мережу, клiєнт Microsoft, клiєнт Netware, сумiсний доступ до файлiв та принтерiв, паролi, вiддалений доступ до мережi, доступ, SNMP, оновлення;
3. система:
4. дозволити створення конфiгурацiй для користувачiв, мережний шлях для встановлення. Windows, мережний шлях до пiдручника, завантажувати при запуску, запускати служби.

Шаблони системних правил. Шаблони - це текстовi файли з певною структурою.

Вiддалене керування.

W97 має засоби, що дозволяють проводити вiддалене керування комп’ютером з W97 з iншого комп’ютера. Основнi функцiї вiддаленого керування: перегляд та модифiкацiя вiддаленого системного реєстру, перегляд завантаження та бiжучої мережної активностi вiддаленого комп’ютера з використанням ‘інспектора мережi’, перегляд параметрiв роботи вiддаленого комп’ютера з використанням системного монiтора, доступ до диску вiддаленого комп’ютера з використанням ‘мережного оточення’. Крiм того, W97 має ряд системних агентiв, якi пристосованi для виконання функцiй керування, архiвування.

Для роботи з вiддаленим керуванням на обох комп’ютерах мусить бути активiзоване вiддалене керування. Дозвiл на проведення керування отримують адмiнiстратори мережi (якщо встановлено доступ на рiвнi користувачiв; список адмiнiстраторiв керування можна змiнити) або фiксується пароль доступу (якщо доступ встановлено на рiвнi ресурсiв).

Для вiддаленого керування бажано встановити доступ на рiвнi користувачiв. Якщо встановлено доступ на рiвнi ресурсiв, деякi утiлiти (редактор реєстру та системних правил, системний монiтор) не будуть доступнi. На обох комп’ютерах мусить бути однаковий тип доступу до ресурсiв. При встановленнi вiддаленого керування створюються два спiльних каталоги: ADMIN$, IPC$. Перший з них надає доступ до файлової системи на вiддаленому комп’ютерi, другий - забезпечує зв’язок мiж процесами на двох комп’ютерах.

Iнсталляцiя та робота з вiддаленим реєстром.

Вiддалений реєстр - це окрема служба, що встановлюється окремо:

**d:\admin\nettools\remotreg**

Вiддалений реєстр працює тiльки в мережах з серверами NT або NETWARE.

Пiсля встановлення служби редагування реєстру операцiї редагування можна проводити засобами редактора системного реєстру та в редакторi системних правил.

Використання ‘інспектора мережi’.

Утiлiта **Netwatch** дозволяє керувати використанням вiддалених комп’ютерiв, дозволяє бачити хто працює з вiддаленим комп’ютером, скiльки вiдкритих файлiв в сеансi. На ПК мусить бути встановлена служба доступу до файлiв. Адмiнiстратор може вiд’єднати користувача вiд вiддаленого комп’ютера, створювати та знищувати каталоги спiльного використання, переглядати список та закривати вiдкритi файли.

Використання системного монiтору.

Встановлене вiддалене керування та служба ‘вiддалений реєстр’. Використовується стандартна програма SYSMON з усiма її можливостями.

Використання ‘мережного оточення’.

Вибiр вiддаленого комп’ютера: Властивостi - Сервiс- Керування. Пiдключення жорсткого диску вiддаленого комп’ютера як C$.

Агенти W97.

1. Агент мережного монiтора Microsoft. Працює як служба. Передає всю iнфомацiю про роботу системи у програму Network monitor WNT. Використовується програма netmon.
2. Агент MIcrosoft SNMP.дозволяє використовувати засоби керування третiх фiрм.
3. Агенти отримання резервних копiй.

**5. Електронна пошта. Microsoft Exchange та Microsoft Fax.**

У W97 можна видiлити наступну iєрархiю поштових служб.

1. Для органiзацiї електронної пошти у межах локальної мережi використовується служба Microsoft Mail.
2. Для роботи пошти у конфiгурацiї з кiлькох локальних мереж з серверами WNT необхiдно встановити на серверi WNT продукт ‘Microsoft Mail Server’.
3. Для виходу в глобальнi мережi можна використати ПЗ пiдключення до MSN (Microsoft Network) або напряму до Internet.

Унiверсальним клiєнтом електронної пошти є Microsoft Exchange (ME). Вiн дозволяє пiдключатись до Compuserve, Microsoft Mail, Internet Mail, MSN. МЕ реалiзується як служба. Крiм МЕ, iснує друга, аналогiчна служба ‘Microsoft Fax’. Особливiстю встановлення цих служб є те, що спочатку встановлюється одна з них. Iнша iнсталюється, як додаткова служба.

Встановлення поштового вiддiлення Microsoft Mail.

Для роботи електронної пошти Microsoft Mail необхiдно спочатку створити поштове вiддiлення (центральне сховище пошти).

Спочатку встановлюється Microsoft Exchange без вказання адреси поштового вiдділення. МЕ встановлюється як продукт у складi W97. Створюється папка Inbox. Вибирається ‘ручне налагодження служб’. Iм’я конфiгурацiї - за замовчуванням. У панелi керування з’являються двi пiктограми - Mail and fax, Microsoft Mail Postoffice.

Розглянемо створення поштового вiдділення. Вказується мiсце розмiщення поштового вiдділення Це - наявний каталог або диск. За визначеною адресою створюєть поштове вiдділення у виглядi папки **WGPO0000**. Ця папка буде мiстити свої каталоги. Введення iнформацiї про адмiнiстратора (iм’я, поштова скринька, пароль). Адмiнiстратор зможе додавати нових користувачiв та виконувати iншi адміністративні функцiї. Перед початком роботи пошти каталог поштового вiддiлення треба визначити, як спiльний ресурс повного використання.

Пiсля створення поштового вiдділення для кожного користувача, який планує користуватись поштою, треба створити облiковий файл.

Встановлення служби Microsoft Mail. Знову встановлюється Microsoft Exchange. Але вказується опцiя ‘вибрати iнформацiйнi служби’. Вказується адреса поштового вiддiлення. Вибирається iм’я зi списку зареєстрованих у поштовому вiддiленнi та пароль. Пiсля цього поштова служба даного користувача вважається встановленою. (iншого користувача можна включити через вiдповiднi профiлi).

Використання Microsoft Exchange.

Запуск МЕ відбувається за пiктограмою Inbox. Запитується пароль доступу до поштового вiддiлення. Якщо користувач ‘кочує’ мiж комп’ютерами, то i свiжа пошта при кожному сеансi пересилається на ПК, з якого входив користувач. Пiсля перемiщення користувача на новий ПК стара пошта не знищується, а залишається ‘хвiст’ з листiв, до яких мають доступ iншi користувачi. Для зняття проблеми треба задати свою Personal Folder на певному мiсцi.

Пiсля входження виводиться список нових листiв. Пункти меню наступні.

Файл. - копiювання та перемiщення повiдомлень мiж папками. Перегляд файлових властивостей повiдомлення. Iмпорт особистих поштових книг та адресних книг.

Редагування помiчених елементiв списку, як прочитаних або непрочитаних.

Вигляд. Створення нових форм екрану. Перегляд всiх папок, вхiдних, вихiдних, вiдправлених та знищених документiв.

Сервiс. Модифiкацiя та конфiгурування функцiй МЕ. Вибiр поштової служби (Microsoft Mail, Microsoft Fax), робота з адресними книгами.

Повiдомлення. Команди щодо роботи з новим повiдомленням. Створення та пересилання.

Для вiдслiдковування зчитування повiдомлення з поштового сервера використовується лiчильник, який декрементується при зчитуванні повiдомлення наступним користувачем. Якщо лiчильник містить 0 - повiдомлення знищується.

Встановлення Microsoft Fax.

Microsoft Fax (MF) дозволяє вiдправляти факси з комп’ютера, а також сумiсно користуватися факсом. Є можливiсть використовувати факс-модеми для вiдправлення та приймання файлiв з використанням технологiї BFT (Binary File Transfer), яка використовується в W97, WKG та iнших системах, що пiдтримують стандарт Microsoft At Work. Використання MF передбачає попереднє встановлення ME. MF встановлюється як продукт у складi W97.

W97 не дозволяє встановлювати MF, якщо встановлена Microsoft Mail та навпаки, але тiльки пiд час встановлення ME. При цьому Microsoft Fax вибирається як iнформацiйна служба. Вказується факс-модем зi списку встановлених. Через опцiю ‘додати’ тут можна вказати або iнший модем, або модем сумiсного використання на iншому ПК (мережний факс-сервер). У випадку звертання до мережного факс-сервера треба вказати UNC-адресу спiльного каталога факса. Крiм того, модем мусить бути визначений, як спiльний. При цьому вказується iм’я користувача, код країни, номер факсу.Якщо МЕ попередньо встановлено, MF додається як нова служба.

**Властивості MF.**

Повiдомлення. Час вiдправлення (якнайскорiше, в конкретний час, за пiльговим тарифом). Формат повiдомлення (з можливiстю редагувати чи нi). Титульна сторiнка.

Набирання номера. Кiлькiсть повторень набирання та iнтервал мiж ними. Властивостi з’єднання (список мiсць з набором властивостей з’єднання для кожного вигiдний для мобiльних користувачiв).

Модем. Вибiр модему та встановлення його спiльного використання. Встановлення кiлькох факс-модемiв та вибiр активного (дiючого в даний момент). Режими набору номера та вiдповiдi.

Користувач. Iнформацiя, що буде з’являтися на титульнiй сторiнцi факса.

Використання Microsoft Fax.

Якщо встановлена служба MF, то можна скласти повiдомлення в МЕ i передати його за адресою, що мiстить номер факсу. При цьому можна приєднувати файли, передавати їх в форматi, що редагується. Можна використовувати факс-сервери. При вказаннi номера можна змiнити параметри модему. Якщо файл посилається не в редактованому форматi, треба вказати його розширення. Тодi вiн вiдсилається у виглядi роздруку свого застосування (наприклад, у форматі Word).

3.6.5. Використання особистої адресної книги.

При створеннi особистої адресної книги можна копiювати в неї фрагменти з загальної поштової книги, а також створювати свої записи. Кiлька користувачiв можуть створити спiльну адресну книгу. Кожний користувач може створити довiльну кiлькiсть спискiв розсилання.

3.6.6. Використання Microsoft Network (MNN).

MNN - це оперативна служба Microsoft. Вона надає послуги електоронної пошти, пiд’єднання до Internet та використання WWW. Вихiд в цю мережу можливий тiльки з W97.

Встановлення MNN.

Запуск - з пiктограми. Двiчi вiдбувається встановлення зв’зку. У перший раз вам передають список бiжучих номерiв доступу. У другий раз - для завершення встановлення i створення облiкового файлу в мережi. Якщо встановлення вiдбувається з мережi, то перший етап вiдбувається тiльки при пiд’єднанні першого ПК. Вказуються телефонні номери. Існує можливiсть вибору параметрiв модему.

Робота з мережею вiдбувається пiд час роботи користувача з Провiдником та МЕ. Завантажується адресна книга MNN.

Через MNN можна отимати доступ i до Internet. Мережа МNN виступає при цьому, як провайдер послуг Internet. Встановлюється Internet Explorer. У ходi встановлення MNN є можливiсть вибрати одну з трьох служб:

1. Microsoft Network;
2. Internet and Microsoft Network;
3. ISDN access to the Internet and MSN.

Тип встановленої служби визначає виключне використання MNN або можливiсть виходу в Internet.

**6. Вiддалений доступ.**

W97 - це ОС, спецiально спроектована з функцiєю вiддаленого доступу. Вона надає мобiльним користувачам можливiсть приєднуватись, як вузол мережi, в будь-який час. Невелика пропускна здатнiсть каналiв зв’язку заставляє перекачувати файлову iнформацiю на вiддалений комп’ютер (не завжди можна працювати в оперативному режимi).

Термiнологiя: комп’ютер, який викликається, називається вiддаленим сервером (dial-up server), а комп’ютер, що викликає, стає вiддаленим клiєнтом (т.ч. це є з’єднанням мiж двома комп’ютерами, а не повноцiнне пiдключення до мережi). Вiддалений сервер W97 пiдтримує одночасно тiльки одного вiддаленого клiєнта. WNT пiдтримує одночасно до 256 клiєнтiв. W97 пiдтримує два типи з’єднань: PPP та SLIP використовуються клiєнтами W97, WNT 3.5, 4, RAS - клiєнтами WKG, WNT 3.1. PPP - багатопротокольний зв’язок. RAS пiдтримує протоколи NETBEUI, SLIP - TCP/IP, NRN (Novell Netware Connect) - IPX/SPX.

Встановлення та налагодження вiддаленого доступу.

Встановлення клiєнта вiдбувається пiд час iнсталяцiї W97. Сервер встановлюється у MPlus! Якщо вiддалений доступ встановлено, то у вiкнi MyComp є папка ‘вiддалений доступ’. Встановлення можна провести через Windows Setup. Компонента вiддаленого доступу має тип мережного адаптера. Це означає, що встановленi мережнi протоколи автоматично прив’язуються до адаптера вiддаленого доступу.

Робота з вiддаленим доступом.

Папка вiдаленого доступу зберiгає заданi з’єднання та має об’єкт ‘нове з’єднання’, вибiр якого дозволяє створити нове з’єднання. При створеннi нового з’єднання вибирається модем, номер вiддаленого сервера, iм’я з’єднання. Властивостi створеного з’єднання можна змiнити, у тому числi вибрати протокол доступу. За замовчуванням встановлюється РРР. Протокол SLIP пiдключається через Windows Setup -> have Disk-> \admin\apptools\dscript\rnaplus.inf. W97 вiдрiзняє мережне з’єднання та з’єднання вiддаленого доступу та використовує спеціальні засоби для боротьби зi зменшенням пропускної здатностi з’єднання вiддаленого доступу.

Налагодження сервера вiддаленого доступу.

Використоваується папка ‘Вiдддалений доступ’- ‘З’єднання’- ‘Сервер вiдаленого доступу’. Вигляд вiкна конфiгурацiї залежить вiд встановленого режиму доступу (щодо ресурсiв або користувачiв). Проводиться заборона (за замовчуванням) або дозвiл вiддаленого доступу, завдання паролю доступу до ресурсiв або списку користувачiв, що мають право доступу, вибiр типу сервера та протоколiв.

Робота з вiддаленим доступом через МЕ.

МЕ аналiзує наявнiсть з’єднання та його тип. Якщо з’єднання немає, можливий вибiр одного з трьох варіантiв:

1. вказати сервер пошти в локальній мережi,
2. використати вiддалений доступ для встановлення з’єднання з поштовим сервером; реально з’єднання буде встановлюватись тiльки при спробi передати данi;
3. не встановлювати з’єднання з поштовим сервером; повiдомлення зберiгаються у черзi i при встановленнi з’єднання з сервером, вiдразу передаються.

Оперативне використання вiддаленого доступу для роботи з поштою.

Вибiр опцiї ‘Remote Mail’ дозволяє вiдкрити дiалогове вiкно для керування пересиланням пошти вiддаленим доступом. Функцiї: пiд’єднання та вiд’єднання вiд сервера, отримання з поштового сервера заголовків повiдомлень, пересилання пошти, робота зi списком вiдправлень.

Пряме з’єднання.

Два ПК з’єднуються через послiдовний або паралельний порти. Один з ПК стає головним (host), другий - пiд’єднаним(guest). Пiд’єднаний комп’ютер має доступ до ресурсiв головного ПК i через нього - вихiд у локальну мережу (головний ПК дiє, як шлюз в мережу тiльки для мереж IPX/SPX та NETBEUI, але не TCP/IP). Встановлення прямого з’єднання - через Windows Setup. Налагодження - завдання статусу ПК, можливостi парольного захисту та паролю. При пiд’єднанні кабелiв пряме з’єднання встановлюється.

Синхронiзацiя файлiв з використанням утiлiти ‘Портфель’.

Портфель - це особливий вид папки, який дозволяє вiдслiдковувати стан скопiйованих в неї файлiв та папок. Портфелiв може бути багато. Портфелi можна перемiщувати на iншi ПК та на дискети. Для вiдслiдковування статусу файлу вiн мусить бути скопiйований, а не перемiщений у портфель. Файл в портфелi може мати статус синхронiзованого та ‘сироти’. Для будь-якого синхронiзованого файлу можливо розiрвати зв’язок з оригiналом. Синхронiзацiя файлiв вiдбувається пiд контролем користувача.

Дистанцiйне керування.

W97 безпосередньо не пiдтримує дистанцiйного керування. Для цього можна використати продукти третiх фiрм (pcAnywhere, Reachout). Дистанцiйне керування працює з бiльшою швидкiстю, але для своєї роботи вимагає окремого ПК в мережi.

***Windows NT***

Універсальна мережева операційна система Windows NT може виконувати роль як клієнта, та і сервера мережі. Термін Windows NT відноситься до двох різних продуктів - Windows NT Workstation і Windows NT Server.

Операційна система Windows NT Workstation оптимізована для використання в якості високопродуктивного захищеного мережевого клієнта і корпоративної операційної системи робочих станцій. Її можна використовувати на автономних комп’ютерах як “персональну” операційну систему, в одноранговій мережі робочої групи і як робочу станцію в середовищі домену Windows NT Server.

Основні переваги Windows NT Workstation:

* **Продуктивність:** підтримка багатозадачності. Windows NT Workstation забезпечує реальну багатозадачність, підтримуючи кілька процесорів.
* **Апаратні профілі:** створення і підтримка списку апаратних конфігурацій даного комп’ютера.
* **Microsoft Internet Explorer:** Web-броузер для роботи з Web.
* **Служба повідомлень (Microsoft Messaging):** прийом і відправка електронної пошти.
* **Служби Web (Peer Web Services):** персональний Web-сервер, оптимізований для роботи під управлінням Windows NT Workstation.
* **Система безпеки:**  забезпечення локального захисту файлів, папок, принтерів та інших ресурсів.
* **Надійність операційної системи:** виконання кожної програми в окремому адресному просторі. Це значить, що некоректно працююча програма не зможе вплинути на роботу інших програм чи операційної системи.

Операційна система Windows NT Server оптимізована для роботи в якості сервера файлів, друку і аплікацій з широким спектром використання: від невеликих робочих груп до корпоративних мереж.

Основні переваги Windows NT Server:

* **Продуктивність сервера:** операційна система Windows NT Server 4.0 оптимізована для досягнення максимальної продуктивності при роботі в якості сервера файлів, друку і аплікацій. Комерційна версія Windows NT Server 4.0 підтримує симетричну багатопроцесорну обробку з використанням до 4 процесорів, а спеціалізовані версії підтримують до 32 процесорів.
* **Вбудовані засоби комунікацій:** дозволяють підключатися до мережі Windows NT Server 4.0 через модем за допомогою сервісу віддаленого доступу (Remote Access Service, RAS). Windows NT підтримує до 256 одночасних сеансів RAS-під’єднань.
* **Засоби управління:**  Task Manager і Network Monitor спрощують адміністрування сервера, надаючи детальну інформацію про кожну програму або процес, що працюють в системі.
* **Internet Information Server (IIS):** - швидка, потужна і безпечна платформа підтримки служб HTTP, FTP, Gopher.
* **Administrative Wizards (Майстри адміністрування):** майстри гранично спрощують управління сервером.
* **Підтримка клієнтів Macintosh:** забезпечує доступ до файлів і принтерів для клієнтів Macintosh.
* **Додаткові мережеві сервіси:** підтримка багатопротокольної маршрутизації (Multiprotocol Routing, MPR), доменної системи імен (Domain Name System, DNS), протоколу динамічної конфігурації хоста (Dynamic Host Configuration Protocol, DHCP) і служби імен Інтернету Windows (Windows Internet Name Service, WINS).
* **Windows NT Directory Services:** база даних домену забезпечує єдину реєстрацію користувачів, централізоване адміністрування домену і доступ до його ресурсів.

Мережі на основі Windows NT організуються на основі доменної моделі або моделі робочої групи. І Windows NT Server і Windows NT Workstation можуть працювати в будь-якій з цих двох моделей.

Доменна модель (domain model) характеризується наявністю в мережі мінімум одного комп’ютера, що працює під управлінням Windows NT Server і виконує роль контролера домену (domain controller). Домен – група комп’ютерів, об’єднаних загальною базою облікових записів користувачів і єдиною політикою захисту. Ця інформація зберігається в базі даних домену (її основна копія знаходиться на комп’ютері – контролері домену).

Модель робочої групи (workgroup model) дозволяє організувати мережу на основі Windows NT без контролера домену. Цю модель часто називають одноранговою мережею (peer-to-peer network), так як всі її комп’ютери мають рівні права на ресурси сумісного використання. Модель робочої групи не забезпечує централізованого адміністрування облікових записів користувачів і захисту ресурсів. Кожен сконфігурований як сервер комп’ютер зберігає інформацію про облікові записи своїх користувачів і захист ресурсів в локальній базі даних.

Захист ресурсів реалізують декілька процесів на різних рівнях операційної системи. Перший з них – *механізм реєстрації* – забезпечує захист доступу до домену або до комп’ютера. При кожному запуску комп’ютера під управлінням Windows NT на екрані виникає вікно з проханням натиснути комбінацію клавіш CTRL+ALT+DELETE для реєстрації в системі. Така реєстрація забезпечує захист від програм, що працюють за принципом “Троянського коня”. Така програма працює під управлінням MS-DOS і дізнається ім’я та пароль користувача, імітуючи вікно Begin Logon. Так як більшість операційних систем використовують CTRL-ALT-DELETE для перезавантаження комп’ютера, то програма-імітатор навряд чи залишиться резидентною при виконанні цієї операції. Для успішної реєстрації в системі користувач повинен ввести коректні значення **User Name**, **Password** і **Domain,** в якому зареєстрований даний користувач.

Зареєструвавшись в системі, можна скористатися комбінацією CTRL-ALT-DELETE для доступу до діалогового вікна Windows NT Security. З його допомогою можна виконати наступні дії:

* **Lock Workstation** – дозволяє заблокувати комп’ютер без виходу з системи. Всі програми при цьому продовжують працювати.
* **Change Password** – дозволяє користувачу змінити пароль свого облікового запису.
* **Logoff –** здійснює вихід користувача з системи.
* **Task Manager –** містить список програм і процесів, які працюють в даний момент. Його можна використовувати для переключення між програмами і для завершення програм, що не реагують на події.
* **Shut Down –** закриває всі файли, зберігає всі дані операційної системи і готує комп’ютер до виключення живлення.
* **Cancel –** закриває діалогове вікно Windows NT Security.

Адміністрування Windows NT передбачає виконання як спеціальних операцій після встановлення системи, так і рутинних повсякденних дій. Функції адміністрування можна розділити на п’ять категорій:

1. **Адміністрування облікових записів користувачів і груп**. Планування, створення і ведення облікових записів і груп для забезпечення кожному користувачу можливості реєстрації в мережі і доступу до необхідних ресурсів.
2. **Адміністрування захисту**. Планування і реалізація стратегії безпеки для захисту даних і загальних мережевих ресурсів, в тому числі папок, файлів і принтерів.
3. **Адміністрування принтерів**. Настройка локальних і мережевих принтерів для забезпечення користувачам доступу до ресурсів друку. Усунення проблем друку.
4. **Моніторинг подій і ресурсів мережі.** Планування і реалізація стратегії аудиту подій в мережі з метою виявлення порушень захисту. Управління ресурсами і контроль їх використання.
5. **Резервне копіювання і відновлення даних.** Планування і виконання регулярних операцій резервного копіювання для забезпечення швидкого відновлення важливих даних.

Засоби адміністрування Windows NT Workstation використовуються тільки для локального комп’ютера. Засоби адміністрування Windows NT Server використовуються для всіх комп’ютерів домену.

Засоби адміністрування встановлюються на Windows NT при установці самої операційної системи:

* **Administrative Wizards**. Інструментальні засоби Windows NT Server для виконання адміністрування: створення облікових записів користувача, створення і зміна облікових записів груп, установка прав доступу до папок і файлів, настройка мережевих принтерів.
* **User Manager for Domains**. Диспетчер користувачів домену – інструментальний засіб Windows NT Server, що дозволяє створювати, знищувати і тимчасово відключати облікові записи користувачів домену. Крім того, він дозволяє задавати стратегію захисту для груп і добавляти до них облікові записи користувачів.
* **User Manager**. Диспетчер користувачів домену – інструментальний засіб Windows NT Workstation, що дозволяє створювати, знищувати і тимчасово відключати локальні облікові записи користувачів і груп.
* **Server Manager.** Диспетчер сервера - інструментальний засіб Windows NT Server для відслідковування комп’ютерів і доменів та управління ними.
* **Event Viewer.** Засіб перегляду подій. Містить відомості про помилки, попередження, а також інформацію про вдалі і невдалі спроби виконання різних дій.
* **Windows NT Diagnostics.** Засоби діагностики, призначені для перегляду і друку інформації про конфігурацію системи.
* **Backup.** Засоби архівування даних призначені для резервного копіювання інформації на локальний носій на магнітній стрічці.

Операційна система Windows NT завжди володіла прекрасними і широко застосовними на практиці можливостями захисту. Однократна реєстрація в домені Windows NT надає користувачам доступ до ресурсів всієї корпоративної мережі.

Повноцінний набір інструментів Windows NT Server полегшує адміністраторам управління системою захисту і її підтримку. Наприклад, адміністратор може контролювати коло користувачів, що мають права доступу до мережевих ресурсів: файлам, каталогам, серверам, принтерам і додаткам. Правами для кожного ресурсу можна управляти централізовано.

Облікові записи користувачів також справляються централізовано. За допомогою простих графічних інструментів адміністратор задає приналежність до груп, допустимий час роботи, термін дії і інші параметри облікового запису. Адміністратор отримує можливість аудиту всіх подій, пов'язаних із захистом доступу користувачів до файлів, каталогів, принтерів і інших ресурсів. Система також здатна блокувати обліковий запис користувача, якщо число невдалих спроб реєстрації перевищує зазделегідь визначене. Адміністратори мають право встановлювати термін дії паролів, примушувати користувачів до періодичної зміни паролів і вибору паролів, що утрудняють несанкціонований доступ.

З точки зору користувача система захисту Windows NT Server повноцінна і нескладна в звертанні. Проста процедура реєстрації забезпечує доступ до відповідних ресурсів. Для користувача невидимі такі процеси, як шифрування пароля на системному рівні. (Шифрування пароля потрібне, щоб виключити передачу пароля у відкритому вигляді по мережі і перешкодити його виявленню при несанкціонованому перегляді мережевих пакетів.) Користувач сам визначає права доступу до тих ресурсів, якими володіє. Наприклад, щоб дозволити спільне використання свого документа, він вказує, хто і як може з ним працювати. Зрозуміло, доступ до ресурсів підприємства контролюється тільки адміністраторами з відповідними повноваженнями.

Більш глибокий рівень безпеки — те, як Windows NT Server захищає дані, що знаходяться в фізичній пам'яті комп'ютера. Доступ до них надається тільки маючим на це право програмам. Так само, якщо дані більше не містяться на диску, система запобігає несанкціонованому доступу до тієї області диска, де вони містилися. При такій системі захисту ніяка програма не «підгляне» у віртуальній пам'яті машини інформацію, з якою оперує в даний момент інший додаток.

Однак інтрамережі швидко стають найбільш ефективним способом спільного використання інформації бізнес-партнерами. Сьогодні доступ до закритої ділової інформації керується створенням облікових записів для нових зовнішніх членів ділової «сім'ї». Це допомагає встановлювати довірчі відносини не тільки з співробітниками корпорації, але і з множиною партнерів.

Віддалений доступ через відкриті мережі і зв'язок підприємств через Інтернет стимулюють постійний і швидкий розвиток технологій безпеки. Як приклад можна виділити сертифікати відкритих ключів і динамічні паролі. Але архітектура безпеки Windows NT однозначно оцінюється як перевершуюча і ці, і інші майбутні технології. Право на таке твердження дають нові можливості і удосконалення, що з'явилися в Windows NT 5.0. Частина цих змін відображає вимоги до захисту великих організацій, інша - дозволяє використати переваги гнучкої архітектури безпеки Windows NT, об'єднаної з сертифікатами відкритих ключів Інтернету.

Перерахуємо нові функції безпеки Windows NT.

**• Інформація про доменні правила безпеки і облікова інформація зберігаються в каталозі Active Directory.** Служба каталогів Active Directory забезпечує тиражування і доступність облікової інформації на багатьох контроллерах домена, а також дозволяє видалене адміністрування.

**• У Active Directory підтримується ієрархічний простір імен користувачів, груп і облікових записів машин.** Облікові записи можуть бути згруповані по організаційних одиницях (що істотно відрізняється від плоскої структури імен в попередніх версіях Windows NT).

**• Адміністративні права на створення і управління групами облікових записів користувачів можуть бути делеговані на рівень організаційних одиниць.** При цьому встановлюються диференційовані права доступу до окремих властивостей призначених для користувача об'єктів. Наприклад, група користувачів може змінювати параметри пароля, але не має доступу до іншої облікової інформації.

**• Тиражування Active Directory дозволяє змінювати облікову інформацію на будь-якому контроллері домена, а не тільки на первинному.** Численні копії Active Directory, що зберігаються на інших (в попередніх версіях, резервних) контроллерах домена, оновлюються і синхронізуються автоматично.

**• Доменна модель змінена і використовує Active Directory для підтримки багаторівневого дерева доменів.** Управління довірчими відносинами між доменами спрощене за рахунок транзитивності в межах всього дерева доменів.

**• У систему безпеки включені нові механізми аутентификації,** такі як Kerberos v5 і TLS (Transport Layer Security), що базуються на стандартах безпеки Інтернету,

**• Протоколи захищених каналів** (SSL 3.0/TLS) **забезпечують підтримку надійної аутентификація клієнта.** Вона досягається шляхом зіставлення мандатів користувачів в формі сертифікатів відкритих ключів з існуючими обліковими записами Windows NT. Для управління обліковою інформацією і контролю за доступом застосовуються одні і ті ж засоби адміністрування, незалежно від того, чи використовується захист з відкритим ключем або із загальним секретом.

**• Додатково до реєстрації за допомогою введення пароля може підтримуватися аутентификація з використанням смарт-карт.** Останні забезпечують шифрування і надійне зберігання закритих ключів і сертифікатів, що особливо важливо для надійної аутентификація при вході в домен з робочої станції.

**• До складу нової версії входить Microsoft Certificate Server.**

Цей сервер призначений для організацій і дозволяє видавати співробітникам і партнерам сертифікати Х.509 версії 3. В CryptoAPI включені інтерфейси і модулі управління сертифікатами відкритих ключів, включаючи видані комерційним ВУС (Уповноваженим сертифікації), стороннім ВУС або Microsoft Certificate Server. Системні адміністратори можуть вказувати, сертифікати яких уповноважених є довіреними в системі і, таким чином, контролювати аутентификація доступу до ресурсів.

**• Зовнішні користувачі, що не мають облікових записів Windows** NT, **можуть бути аутентифіковані за допомогою сертифікатів відкритих ключів і співвіднесені з існуючим обліковим записом.** Права доступу, призначені для цього облікового запису, визначають права зовнішніх користувачів на доступ до ресурсів.

• У розпорядженні користувачів **засоби управління парами закритих (відкритих) ключів і сертифікатами, що використовуються** для доступу до ресурсів Інтернету.

**• Технологія шифрування вбудована в операційну систему** і дозволяє використати цифрові підписи для ідентифікації потоків.

У Windows NT 5.0 вбудований сервер сертифікатів Certificate Server, який може видавати сертифікати в стандартних форматах (Х.509 версій 1 і 3), а також додавати розширення по мірі потреби.

**Протокол аутентификації Kerberos**

Протокол аутентификації Kerberos визначає взаємодію між клієнтом і мережевим сервісом аутентификації, відомим як KDC (Key Distribution Center). У Windows NT KDC використовується як сервіс аутентификація на всіх контроллерах домена. Домен Windows NT еквівалентний області *Kerberos*, але до неї звертаються як до домену. Реалізація протоколу Kerberos в Windows NT заснована на визначенні Kerberos в RFC1510, Клієнт Kerberos реалізований у вигляді ПФБ (постачальника функцій безпеки) Windows NT, заснованому на SSPI. Початкова аутентификація Kerberos інтегрована з процедурою WinLogon. Сервер Kerberos (KDC) інтегрований з існуючими службами безпеки Windows NT, що виконуються на контроллері домена. Для зберігання інформації про користувачів і групи він використовує службу каталогів Active Directory.

Протокол Kerberos посилює існуючі функції безпеки Windows NT і додає нові. Розглянемо останні детальніше.

**• Підвищена швидкість аутентификації при встановленні початкового з'єднання.** Сервер додатків не повинен звертатися до контроллера домена для аутентификація клієнта. Така конфігурація підвищує масштабованість серверів додатків при обробці запитів на підключення від великого числа клієнтів.

**• Делегування аутентификації в багатоярусній архітектурі клієнт-сервер.** При підключенні клієнта до сервера, останньому імперсонує (втілює) клієнта в цій системі. Але якщо серверу для завершення транзакції треба виконати мережеве підключення до іншого сервера, протокол Kerberos дозволяє делегувати аутентификації першого сервера і підключитися до другого від імені клієнта. При цьому другий сервер також виконує імперсонацію клієнта.

**• Транзитивні довірчі відносини для міждоменної аутентификації.** Користувач може бути аутентифікований в будь-якому місці дерева доменів, оскільки сервіси аутентификації (KDC) в кожному домені довіряють квиткам, виданим іншими KDC в дереві. Транзитивне довір'я спрощує управління доменами у великих мережах з декількома доменами.

**Аутентификація NTLM**

Перед тим, як розглянути процес аутентификації Kerberos, пригадаємо механізм, діючий в попередніх версіях Windows NT.

Отже, після того, як користувач вводить своє ім'я і пароль, система аутентифікує його шляхом передачі параметрів, заданих у ввідному діалоговому вікні, менеджеру захисту облікових записів SAM (Security Account Manager). SAM порівнює ім'я користувача і зашифрований пароль з тими, що зберігаються в базі користувачів домена або, при локальній реєстрації, робочій станції. Якщо ім'я і пароль співпадають, сервер повідомляє робочу станцію про підтвердження доступу. Крім того, сервер завантажує і таку інформацію про користувача, як привілей облікового запису, положення домашнього каталога і т. п. Якщо для користувача визначений сценарій реєстрації, цей сценарій також завантажується на робочу станцію для виконання.

Якщо користувач має обліковий запис і привілеї доступу в систему, а введений ним пароль вірний, підсистема захисту створює об'єкт *маркер доступу,* що представляє користувача. Він порівняємо з ключем, що містить «посвідчення особи» користувача. Маркер доступу зберігає таку інформацію, як ідентифікатор захисту SID (Security ID), ім'я користувача і імена груп, до яких він належить.

Маркер доступу або його копія асоціюються з будь-яким процесом, що виконується користувачем (наприклад, відкриття або друк файла). Комбінація процес-маркер називається суб'єктом*. Суб'єкти* оперують над об'єктами Windows NT шляхом виклику системних сервісів. Коли суб'єкт здійснює доступ до захищеного об'єкта, (наприклад, файлу або каталогу), вміст маркера порівнюється з вмістом списку контролю доступу до об'єкта ACL (Access Control List) шляхом стандартної перевірки. При цьому визначається, чи можна надати суб'єкту право на виконання операції, що запитується. Ця ж процедура може при необхідності згенерувати повідомлення аудиту, що відображають результати спроб доступу.

Створений маркер передається процесу Win32 WinLogon. WinLogon наказує підсистемі Win32 створити процес для користувача, і маркер доступу приєднується до цього процесу. Після цього підсистема Win32 ініціює Windows NT Explorer, і на екрані з'являється відповідне вікно.

**Основи Kerberos**

Kerberos є протоколом аутентификації з спільним секретом - і користувачеві, і KDC відомий пароль (KDC зашифрований 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 отримує початковий квиток Kerberos TGT (Ticket grant ticket), заснований на зашифрованому представленні пароля. Windows NT зберігає TGT в 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 вірний квиток для поточного сеансу роботи з сервером. Якщо такого квитка немає, на KDC посилається запит з TGT для отримання сеансового квитка, що дозволяє доступ до сервера.

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

Сеансовий квиток Kerberos пред'являється видаленій службі в повідомленні про початок підключення. Частини сеансового квитка зашифровані секретним ключем, що використовується спільно службою і KDC. Сервер може швидко аутентифікувати клієнта, перевіривши його сеансовий квиток і не звертаючись до сервісу аутентификації, оскільки на сервері в кеші зберігається копія секретного ключа. З'єднання при цьому відбувається набагато швидше, ніж при аутентификації NTLM, де сервер отримує мандати користувача, а потім перевіряє їх, підключившись до контроллера домена.

Сеансові квитки Kerberos містять унікальний сеансовий ключ, створений KDC для симетричного шифрування інформації про аутентификацію, а також даних, що передається від клієнта до сервера. У моделі Kerberos KDC використовується як інтерактивна довірена сторона, що генерує сеансовий ключ.

**Інтеграція Kerberos**

Протокол Kerberos повністю інтегрований з системою безпеки і контролю доступу Windows NT. Початкова реєстрація в Windows NT забезпечується процедурою WinLogon, що використовує ПФБ Kerberos для отримання початкового квитка TGT. Інші компоненти системи, наприклад, Redirector, застосовують інтерфейс SSPI до ПФБ Kerberos для отримання сеансового квитка для видаленого доступу до файлів сервера SMB.

У протоколі Kerberos версії 5 для сеансових квитків визначено поле, що шифрується. Воно призначене для даних авторизації, однак використання цього поля визначається конкретними додатками, В Windows NT полі даних авторизації служить для зберігання ідентифікатора безпеки Security ID, що однозначно визначає користувача і членство в групі. Постачальник функцій безпеки Kerberos на серверний стороні використовує поле авторизації для створення *маркера захищеного доступу (security access token), що представляє* користувача в цій системі. Сервер, слідуючи моделі безпеки Windows NT, використовує цей маркер для доступу до локальних ресурсів, захищених списками контролю доступу.

Делегування аутентификації підтримується в протоколі Kerberos версії 5 шляхом використання в сеансових квитках прапорів proxy і forwarding. Сервер Windows NT застосовує делегування для отримання сеансового квитка на доступ від імені клієнта до іншого сервера.

**Взаємодія Kerberos**

Протокол Kerberos версії 5 реалізований в різних системах і використовується для одноманітності аутентификація в розподіленій мережі.

Під взаємодією Kerberos мається на увазі загальний протокол, що дозволяє обліковим записам аутентифікованих користувачів, що зберігаються в одній базі (що можливо тиражується) на всіх платформах підприємства, здійснювати доступ до всіх сервісів в гетерогенного середовищі. Взаємодія Kerberos засновується на наступних характеристиках:

• загальний протокол аутентификації користувача або сервісу на основне ім'я при мережевому підключенні;

• можливість визначення довірчих відносин між областями Kerberos і створення посилальний запитів квитків між областями;

• підтримка певних вимог в RFC 1510 до взаємодії, що відносяться до алгоритмів шифрування і контрольних сум, взаємної аутентификація і інших можливостей квитків;

• підтримка форматів маркера безпеки Kerberos версії 5 для встановлення контексту і обміну повідомленнями так, як це визначене робочою групою lETFCommon Authentication Technology.

**Підтримка Kerberos відкритих ключів**

У Windows NT також реалізовані розширення протоколу Kerberos, підтримуючий додатково до аутентификацію з секретним загальним ключем використовується аутентификація, засновану на парах відкритого (закритого) ключа. Підтримка відкритих ключів дозволяє клієнтам запитувати початковий ключ TGT за допомогою закритого ключа, в той час як KDC перевіряє запит за допомогою відкритого ключа, отриманого з сертифіката Х.509 (зберігається в призначеному для користувача об'єкті в каталозі Active Directory), Сертифікат користувача може бути виданий як стороннім уповноваженим сертифікації (Certification Authority), так і Microsoft Certificate Server, що входить в Windows NT. Після початкової аутентификація закритим ключем використовуються стандартні протоколи Kerberos для отримання сеансових квитків на доступ до мережевих служб,

Підтримка протоколом Kerberos відкритих ключів - основа аутентификація в мережі за допомогою смарт-карт. Користувачі Windows NT 5.0 можуть їх застосовувати для входу в систему.

**Сервер сертифікатів Microsoft Certificate Server**

Сервер сертифікатів Microsoft Certificate Server надає організаціям спрощений, без звернення до зовнішніх ВУС (уповноваженим сертифікації), процес видачі сертифікатів. З його допомогою досягається повний контроль над правилами видачі, управління і відгуку сертифікатів, а також над форматом і змістом самих сертифікатів. Реєстрація всіх транзакцій дозволяє адміністратору відстежувати запити на видачу сертифікатів і управляти ними.

Certificate Server виконується у вигляді сервісу Windows NT і обробляє всі запити сертифікатів, випадки їх видачі, а також всі списки відгуку. Статус кожної операції з сертифікатами відстежується за допомогою черги транзакцій. По завершенні операції інформація про неї заноситься в журнал транзакцій для подальшої перевірки адміністратором.

**Клієнт і вхідний модуль**

Запит сертифіката поступає від будь-якого, підтримуючого цифрові сертифікати, клієнтського додатку. Це можливо, наприклад, програма перегляду сторінок Web, поштовий клієнт або клієнт електронного магазина. Точку входу Certificate Server - так званий *вхідний модуль* можна настроїти на прийом запитів в багатьох стандартних форматах. Вхідні модулі виконують дві основні функції: розпізнають протокол або транспортний механізм, що використовується запитуючим додатком, а також встановлюють з'єднання з сервером сертифікатів для передачі запитів. Якщо треба забезпечити так специфічні потреби, що це не під силу вхідним модулям, що поставляються, можна написати свій власний модуль, використовуючи інтерфейс СОМ, що надається Certificate Server.

**Модуль черг і правил**

Вхідний модуль передає запит у виконавчу частину сервера сертифікатів, де відбувається введення запиту в чергу, а далі передача в модуль правил. Саме там на основі додаткової інформації, що міститься в запиті визначається можливість видачі запитаного сертифіката. Так само, як і вхідний модуль, модуль правил є повністю таким, що настроюється.

У процесі прийняття рішення про видачу сертифіката, модуль правил може звернутися до зовнішніх баз даних, таких як каталог Active Directory, або успадкована база даних, або кредитна інформація від стороннього джерела, щоб перевірити надану інформацію. Також він може посилати адміністраторам попередження про необхідність видачі їм дозволи.

Після цього інформація упаковується в запит так, як вказана адміністратором. Модуль правил може бути настроєний на вставку будь-яких розширень сертифікатів, що зажадалися клієнтським додатком (наприклад, дані для оцінки купівельних можливостей клієнта).

Коли модуль правил повертає запит на надання сертифіката назад у виконавчий модуль, оновлюються черга, шифрування і цифровий підпис сертифіката, а також запис транзакції. У журнал заносяться не тільки всі запити, але і те, чи були вони задоволені або знехтувані. Там же з метою подальшого аудиту зберігаються всі видані сертифікати і списки відгуку сертифікатів.

Certificate Server передає сертифікат у вихідний модуль, який упаковує його у відповідний транспортний механізм або протокол. Так, сертифікат може бути переданий поштою, по мережі або вміщений в службі каталогів, наприклад, Active Directory.

Подібно вхідному модулю, вихідного також повністю настроюємо. Більш того в одному сервері допустимі декілька вихідних модулів, і один і той же сертифікат може бути не тільки відправлений клієнту, але і вміщений, наприклад, в репозитарій сертифікатів для подальшого використання (в тому числі для перевірки інформації в призначеному для користувача сертифікаті).

Для конфігурування, моніторинга і управління операціями на сервері в склад Certificate Server включений ряд адміністративних інструментів. Вони дозволяють модифікувати правила, додавати нові вхідний і вихідний модулі, переглядати чергу. Переглядаючи чергу, адміністратор може або відкинути запит про сертифікат або, навпаки, ініціювати його негайну видачу.

**Безпека і Active Directory**

У всіх попередніх версіях Windows NT інформація про облікові записи зберігалася в захищених гілках реєстру на контроллерах домена. Довірчі відносини між доменами і наскрізна аутентификація в дворівневих ієрархіях доменів дозволяли досить гнучко управляти обліковими записами і серверами ресурсів. Однак всередині кожного домена простір імен був плоским і не мав ніякої внутрішньої організації.

Розподілені служби безпеки Windows NT 5.0 використовують Active Directory як сховище облікової інформації. Active Directory значно перевершує реєстр по продуктивності і масштабованості. Особливо вражають її адміністративні можливості.

Розглянемо переваги інтегрованого управління обліковими записами службою каталогів Active Directory.

**• Облікові записи користувачів, груп і машин можуть бути організовані у вигляді контейнерів каталога,** званих, як вже згадувалося, організаційними одиницями OU. У домені допустиме довільне число OU, організованих у вигляді деревовидного простору імен у відповідності зі структурою організації користувача. Також як і OU, облікові записи окремих користувачів є об'єктами каталога. При зміні співробітниками місця роботи або посади облікові записи всередині дерева доменів можуть бути легко переміщені, і, таким чином, приведені у відповідність з новим положенням.

**• Каталог Active Directory дозволяє враховувати набагато більше об'єктів користувачів, ніж реєстр.** Розмір одного домена вже не обмежений продуктивністю сервера, що зберігає облікові записи. Дерево пов'язаних між собою доменів Windows NT може підтримувати великі і складні організаційні структури.

**• Адміністрування облікової інформації розширене за рахунок графічних коштів управління Active Directory, а також за рахунок підтримки OLE DS в мовах сценаріїв.** Загальні задачі адміністрування можуть бути вирішені у вигляді сценаріїв, що дозволяє автоматизувати їх виконання.

**• Служба тиражування каталогів дає можливість мати декілька списів облікової інформації,** причому оновлюватися ця інформація може в будь-якій копії, а не тільки на виділених первинних контроллерах домена. Протокол LDAP і синхронізація каталогів забезпечують механізми зв'язку каталога Windows NT з іншими каталогами на підприємстві.

Зберігання облікової інформації в Active Directory означає, що користувачі і групи представлені там у вигляді об'єктів каталога. Права на читання і запис можуть бути надані окремим особам, як по відношенню до всього об'єкта цілком, так і по відношенню до окремих його властивостей. Адміністратори можуть точно задавати, хто саме правомочний модифікувати інформацію про користувачів, і яку саме. Наприклад, оператору телефонної служби дозволяється змінювати інформацію про телефонні номери користувачів, але при цьому він не володіє привілеями системного оператора або адміністратора.

Поняття груп спростилося, і місце локальних і глобальних груп тепер займають просто *об'єкти гpynn. З* їх допомогою можна управляти як доступом до ресурсів в масштабі всього домена, так і до локальних ресурсів контроллера домена.

Між Active Directory і службами безпеки Windows NT існують фундаментальні відносини. У Active Directory зберігаються правила безпеки домена, що визначають порядок використання системи (обмеження паролів, обмеження на доступ до системи і інш.). Об'єкти каталога, що відносяться до безпеки, повинні бути захищені від несанкціонованого доступу. У Windows NT реалізована об'єктна модель безпеки і контролю за доступом до всіх об'єктів в каталозі Active Directory. У кожного об'єкта є свій унікальний дескриптор захисту, що визначає дозволи на читання або оновлення властивостей об'єкта.

Для визначення прав даного клієнта прочитувати або модифікувати певний об'єкт в Active Directory служить імперсонація і верифікація доступу Windows NT. Іншими словами, при надходженні LDAP-запита від клієнта доступ до об'єктів каталога контролюється операційною системою, а не службою каталогів Active Directory.

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

**Довірчі відносини між доменами**

У Windows NT 5.0 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, що входять в дерево.

Явні відносини довір'я встановлюються не тільки з доменами старого типу, але і в тому випадку, коли неявні двосторонні відносини не придатні для використання: наприклад, для домена фінансового відділу або бухгалтерії. Встановлення явних односторонніх довірчих відносин автоматично відміняє неявні довірчі відносини Kerberos.

Проте, у великій організації явні односторонні відносини потрібні не так уже часто. Неявні двосторонні довірчі відносини значно полегшують управління обліковими записами з декількох доменів, оскільки всі домени в дереві неявно довіряють один одному.

**Делегування адміністративних повноважень**

Делегування адміністративних повноважень - гнучкий інструмент обмеження адміністративної діяльності рамками частини домена. Цей метод дозволяє надати окремим співробітникам можливість управління користувачами або групами в заданих межах і, в той же час, не дає їм прав на управління обліковими записами, що відносяться до інших підрозділів.

Права на визначення нових користувачів або створення груп користувачів делегуються на рівні OU або контейнера, в якому створений обліковий запис. Адміністратори груп однієї організаційної одиниці не завжди мають можливість створювати облікові записи того ж самого домена, що відносяться до іншої організаційної одиниці або управляти ними. Однак доменні правила і права доступу, визначені на більш високих рівнях каталога, можуть бути застосовані по всьому дереву за допомогою механізму успадкування.

Існує три способи делегування адміністративних повноважень:

• на зміну властивостей певного контейнера, наприклад, LocalDomainPolicies самого домена;

• на створення і видалення дочірніх об'єктів певного типу (користувачі, групи, принтери і ін.) всередині OU;

• на оновлення певних властивостей деяких дочірніх об'єктів всередині OU (наприклад, право встановлювати пароль для об'єктів типу User).

Делегувати повноваження просто. Досить вибрати особу, якій будуть делеговані повноваження, і указати, які саме повноваження передаються. Інтерфейс програми адміністрування Active Directory дозволяє без ускладнень переглядати інформацію про делегування, визначену для контейнерів.

**Детальне призначення прав доступу**

Звичайно у великій організації за забезпечення безпеки і підтримки інфраструктури мережі відповідають декілька чоловік або груп. Отже, повинна існувати можливість надавати таким особам або групам права на виконання певних операцій без права створення додаткових облікових записів і впливу на властивості інших облікових записів.

Архітектурою безпеки об'єктів Active Directory використовуються дескриптори захисту Windows NT для контролю за доступом до об'єктів. Кожний об'єкт в каталозі має унікальний дескриптор захисту. Вхідний в дескриптор список контролю доступу ACL (Access Control List), містить рядки, що визначають дозвіл або заборону на певні види доступу для окремих осіб або груп. Права доступу можуть бути надані або заборонені в різній мірі. Існують рівні прав доступу, що розрізнюються застосуванням до:

• об'єкту загалом (при цьому зачіпаються всі властивості об'єкта);

• групі властивостей, визначеній наборами властивостей всередині об'єкта;

• окремій властивості об'єкта.

За умовчанням доступ для читання і запису до всіх властивостей об'єкта отримує творець об'єкта.

Заборона або надання доступу до групи властивостей зручна для визначення родинних властивостей. Групування властивостей виконується відповідним атрибутом властивості в схемі. Взаємовідносини наборів властивостей можна змінювати, модифікуючи схему.

Нарешті, призначення прав доступу до окремих властивостей являє собою найвищий рівень деталізування, застосовний до всіх об'єктів Active Directory.

Контейнерні об'єкти в каталозі також підтримують детализація доступу, регламентуючи, хто має право створювати дочірні об'єкти і якого типу. Наприклад, правило доступу, визначене на рівні організаційної одиниці, може визначати, хто має право створювати об'єкти типу User (користувачі) в цьому контейнері. Інше правило в цієї ж OU може визначати, хто має право створювати об'єкти типу Printer.

**Успадкування прав доступу**

Успадкування прав доступу означає, що інформація про управління доступом, визначена у вищих шарах контейнерів в каталозі, розповсюджується нижче на вкладені контейнери і об'єкти-листя. Існують дві моделі успадкування прав доступу: *динамічна* і *статична.* При динамічному успадкуванні права визначаються шляхом оцінки дозволів на доступ, призначених безпосередньо для об'єкта, а також для всіх батьківських об'єктів в каталозі. Це дозволяє ефективно управляти доступом до частини дерева каталога, вносячи зміни в контейнер, що впливає на всі вкладені контейнери і об'єкти-листя. Зворотна сторона такої гнучкості недостатньо висока продуктивність через час визначення ефективних прав доступу при запиті користувача.

У Windows NT реалізована статична форма успадкування прав доступу, іноді також звана *успадкуванням в момент створення.* Інформація про управління доступом до контейнера розповсюджується на всі вкладені об'єкти контейнера. При створенні нового об'єкта успадковані права зливаються з правами доступу, що призначаються за умовчанням. Будь-які зміни успадкованих прав доступу, дерева, що виконуються надалі на вищих рівнях, повинні розповсюджуватися на всі дочірні об'єкти. Нові успадковані права доступу розповсюджуються на об'єкти Active Directory відповідно до того, як ці нові права визначені. Статична модель успадкування дозволяє збільшити продуктивність.

Аудит

Аудит одне з засобів захисту мережі Windows NT. З його допомогою можна відстежувати дії користувачів і ряд системних подій в мережі. Фіксуються наступні параметри, що стосуються дій, що здійснюються користувачами:

1. виконана дія;
2. ім'я користувача, що виконав дію;
3. дата і час виконання.

Аудит, реалізований на одному контроллері домена, розповсюджується на всі контроллери домена. Настройка аудиту дозволяє вибрати типи подій, що підлягають реєстрації, і визначити, які саме параметри будуть реєструватися.

У мережах з мінімальним вимогам до безпеки піддавайте аудиту:

1. успішне використання ресурсів, тільки в тому випадку, якщо ця інформація вам необхідна для планування;
2. успішне використання важливої і конфіденційної інформації.

У мережах зі середніми вимогами до безпеки піддавайте аудиту:

1. успішне використання важливих ресурсів;
2. вдалі і невдалі спроби зміни стратегії безпеки і адміністративної політики;
3. успішне використання важливої і конфіденційної інформації.

У мережах з високими вимогами до безпеки піддавайте аудиту:

1. вдалі і невдалі спроби реєстрації користувачів;
2. вдале і невдале використання будь-яких ресурсів;
3. вдалі і невдалі спроби зміни стратегії безпеки і адміністративної політики.

Аудит приводить до додаткового навантаження на систему, тому реєструйте лише події, що дійсно представляють інтерес.

Windows NT записує події в три журнали:

1. *Системний журнал (*system log) містить повідомлення про помилки, попередження і іншу інформацію, вихідну від операційної системи і компонентів сторонніх виробників. Список подій, що реєструються в цьому журналі, приречений операційною системою і компонентами сторонніх виробників і не може бути змінений користувачем. Журнал знаходиться в файлі Sysevent.evt.
2. *Журнал безпеки (*Security Log) містить інформацію про успішні і невдалі спроби виконання дій, що реєструються засобами аудиту. Події, що реєструються в цьому журналі, визначаються заданою вами стратегією аудиту. Журнал знаходиться в файлі Secevent.evt.
3. *Журнал додатків (*Application Log) містить повідомлення про помилки, попередження і іншу інформацію, що видається різними додатками. Список подій, що реєструються в цьому журналі, визначається розробниками додатків. Журнал знаходиться в файлі Appevent.evt.

Всі журнали розміщені в папці %Systemroot%\System32\Config

ЕЛЕМЕНТИ БЕЗПЕКИ СИСТЕМИ Windows NT

**Облікові записи користувачів і груп**

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

Так само, як і в попередніх версіях Windows NT, у версії 5.0 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, фіксуючий мінімальні привілеї гостя;

**• *Administrator*** вбудований обліковий запис для користувачів, наділених максимальними привілеями;

**• *Krbtgt*** вбудований обліковий запис, що використовується при початковій аутентификація Kerberos.

Крім них є два приховані вбудовані облікові записи:

**• *System*** обліковий запис, що використовується операційною системою;

**• *Creator owner*** творець (файла або каталога).

Перерахуємо вбудовані групи:

***• локальні (залишені для сумісності)***

Account operators;

Administrators;

Backup operators;

Guests;

Print operators;

Replicator;

Server operators;

Users;

***• і глобальні***

Domain guests гості домена;

Domain Users користувачі домена;

Domain Admins адміністратори домена.

***Крім цих вбудованих груп є ще ряд спеціальних груп:***

• Everyone в цю групу за умовчанням включаються взагалі всі користувачі в системі;

• Authenticated users в цю групу включаються тільки аутентифицированние користувачі домена;

• Self сам об'єкт.

**Домени Windows NT**

Управління доменами здійснюється за допомогою адміністративної консолі DNS. Ви можете визначити зони, прописати повністю певні імена, включити в домени комп'ютери і т. п.

Як вже вказувалося, домени об'єднуються в дерева. Для перегляду дерева доменів використовується спеціальний зліпок консолі управління (domain.msc), званий Domain Tree Management.

Встановлення довірчих відносин явного типу нічим не відрізняється від того, що застосовувався в попередніх версіях: у верхній список заносяться імена доменів, яким довіряє даний домен; а в нижній імена доменів, які можуть йому довіряти.

Як вже вказувалося, ці довірчі відносини є значення задавати лише тоді, коли двостороннє транзитивне довір'я Kerberos, що встановлюється за умовчанням, не відповідає безпеці; а також у разі зв'язку між кореневими доменами дерев в лісі.

Домени можуть працювати в двох режимах: «рідному» (native) і змішаному (mixed). При роботі в змішаному режимі в домен можуть входити як контроллери доменів, на яких встановлена версія Windows NT 5.0, так і з більш ранніми версіями.

«Рідний» режим роботи допускає включення в домен тільки контроллерів домена з Windows NT 5.0. У цьому режимі з'являється можливість створення вкладених груп, а також междоменного членства в групі.

Інформація про домене являє собою набір властивостей доменного об'єкта. Серед властивостей є *обов'язкові,* наприклад, ім'я домена. А ось інформація про адміністратора домена - *необов'язкова.* З точки зору забезпечення працездатності вона не має ніякого значення і тому цілком може бути опущена. Однак передбачимо, що Ви бажаєте знайти в дереві всю домени, якими управляє адміністратор Петров. Якщо інформація, показана на малюнку, не була введена завчасно, то поставлена задача зможе бути вирішена тільки шляхом особистого звернення до адміністратора Петрову.

Оскільки домен є контейнерним об'єктом каталога Active Directory, до нього застосовні ті ж самі види доступу, що і до будь-якого контейнера: повний доступ, читання, запис, створення і видалення дочірніх об'єктів.

**Локальна політика безпеки**

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

У порівнянні з можливостями аудиту, що були в Windows NT 4.0, в нової версії ОС доданий аудит ще двох категорій подій. Це специфічні події, пов'язані з доступом до служби каталогів Active Directory, і події, що відносяться до аутентификація Kerberos. Доступний роздільний аудит успішних і неуспішних подій.

**Доменна політика**

Доменна політика встановлює правила для всіх облікових записів в домені, торкаючись такі сфери, як правила паролів, блокування облікових записів, вибір уповноважених безпеці, Kerberos-правила і т. д. В першої бети-версії реалізовані тільки правила паролів і блокування облікових записів. По своїх можливостях вони практично не відрізняються від правил попередньої версії Windows NT.

Якщо пароль користувача довгий час незмінний, 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 умовчанням тривалість дії пароля 42 дні.

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

За умовчанням *довжина пароля користувача* варіюється від 0 до 14 символів. Зрозуміло, що при підвищених вимогах до захищеності системи пустий пароль недопустимо. У цьому випадку адміністратор системи призначає мінімальну довжину пароля. Створюючи новий обліковий запис для користувача, адміністратор може указати пароль довільної довжини, незалежно від обмеження, заданого політикою ведення облікових записів. Однак якщо пароль змінюється користувачем після реєстрації в системі, то параметри нового пароля повинні точно відповідати політиці ведення облікових записів.

Обмеження *мінімально можливого терміну зміни пароля* користувачем доцільне, наприклад, якщо в системі працює багато починаючих користувачів. По-перше, певний термін дає користувачам, що недавно познайомилися з Windows NT, можливість звикнути до особливостей захищеної роботи і пересвідчитися в необхідності пам'ятати свій пароль. По-друге, починаючий користувач, змінивши після закінчення терміну дії пароль, може захотіти повернутися до колишнього. Але зробити це і ослабити таким чином захищеність системи не дозволить примусова затримка. Це особливо ефективне, якщо встановити параметр *відстеження унікальності пароля.*

Мінімальний період для дозволу зміни пароля варіюється в межах від 1 до 999 днів. За умовчанням він не обмежується. Звичайно, досить встановити 14 днів.

**Редактор конфігурацій безпеки**

Однак при автоматичній установці операційних систем на велике число комп'ютерів, при адмініструванні великих корпоративних мереж всі ці інструменти, незважаючи на свою корисність, стають недостатньо ефективними, що загалом приводить до підвищення вартості адміністрування. Для роботи в таких умовах необхідний принципово інший метод, що об'єднує в собі можливості всіх згаданих інструментів. Тільки так можна гарантувати ефективну політику безпеки і контроль захисту в масштабах великого підприємства.

У ролі такого інструмента успішно виступає *редактор конфігурацій безпеки.* Питання, пов'язані із забезпеченням безпеки, можна умовно розділити на декілька областей. Microsoft ідентифікував і представив в редакторі конфігурацій безпеки лише деякі області, що ні в якій мірі не обмежує Вас в ідентифікації і доданні в редактор нових областей.

За замовченням підтримуються наступні області безпеки:

**• політика безпеки**  завдання різних атрибутів безпеки на локальному і доменному рівнях; так само охоплює деякі установки на машинному рівні;

**• управління групами з обмеженнями**  дозволяє управляти членством в групах, які, на думку адміністратора, «чутливі» з точки зору 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 каталога 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 образом дають можливість незалежним виробникам програмного забезпечення розширювати редактор конфігурацій безпеки для усунення специфічних проблем.

**Функції редактора конфігурацій безпеки**

Редактор конфігурацій безпеки зліпок консолі управління ММС. Розглянемо його основні функції.

**• Визначення шаблонів конфігурацій безпеки.** Якщо Ви прагнете забезпечити безпеку в масштабах підприємства, що нараховує сотні або тисячі комп'ютерів, найкраще скористатися шаблонами замість індивідуальної настройки кожної машини. Передбачимо, що всі комп'ютери можуть мати десять різних варіантів настройки параметрів захисту. У такому випадку, зручно зробити десять шаблонів, кожний з яких буде відповідати своєму варіанту захисту, і застосовувати ці шаблони відповідно до потреб. Коли Ви застосовуєте шаблон, в реєстр комп'ютера вносяться зміни, які і визначають настройки 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 файла в редактор конфігурацій ці параметри відображаються в зручному для аналізу і редагування вигляді. Редактор також дозволяє створювати нові файли-шаблони.

**• Конфігурування системної безпеки.** Для конфігурування параметрів системної безпеки можна або вибрати відповідну команду в меню завантаженого зліпка (що приведе до запису параметрів з шаблона в реєстр), або скористатися версією редактора, що виконується з командного рядка. При другому варіанті виклик редактора можна вбудувати в адміністративний сценарій, який буде виконаний або негайний, або в будь-який зручний для Вас час.

**• Аналіз системної безпеки.** Аналіз параметрів, порівняння їх із заданими, що забезпечують певний рівень захисту, не менш важливий, ніж власне настройка. Так, в Windows NT Resource Kit 4.0 входить утиліта, що дозволяє на основі аналізу настройок системи робити висновок про відповідність захисту рівню С2. Редактор конфігурацій безпеки дає можливість порівнювати настройки з шаблоном. Виконується ця операція або за допомогою відповідної команди меню редактора, або запуском з командного рядка.

**• Перегляд результатів аналізу.** Редактор дозволяє переглядати результати порівняння існуючої конфігурації з шаблонною, в тому числі з використанням виразних графічних коштів.