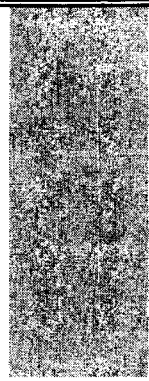
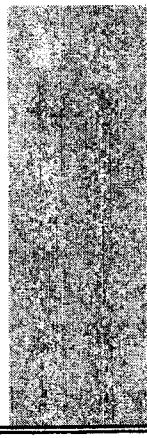
AZƏRBAYCAN MİLLİ ELMLƏR AKADEMİYASI
İNFORMASİYA TEXNOLOGİYALARI İNSTİTUTU



Rəhimov E.R.

KORPORATİV ŞƏBƏKƏLƏRİN İDARƏ EDİLMƏSİ



Bakı - 2008

ISBN 978-9952-434-08-8

Xülasə:

Kitabda korporativ şəbəkələrin idarə olunmasının əsas aspektləri və texniki imkanları ətraflı nəzərdən keçirilmişdir. Beynəlxalq standartları nəzərə alaraq müəlliflər tərəfindən korporativ şəbəkələrin idarə olunmasının daha effektiv və təhlükəsiz olması üçün bir sıra təkliflər və tövsiyələr toplusu verilmişdir. Həmçinin ixtiyari korporativ şəbəkələrin layihələndirilmə mərhələsində informasiya təhlükəsizliyinin qiymətləndirilməsinə imkan verən riyazi metod işlənib hazırlanmışdır. Kitab müxtəlif arxitekturaya malik korporativ şəbəkələrin idarə olunmasına imkan verən instrumental vasitələrin, platformaların və sistem xidmətlərin tam texniki şərhi və imkanlarını izah edir.

Bu səbəbdən kitab müxtəlif oxucular üçün, administratorlar, kompüter və ya şəbəkə mütəxəssisləri və bu ixtisasın tədrisi ilə məşğul olan müəllimlər və tələbələr üçün nəzərdə tutulmuşdur.

Müəlliflər:

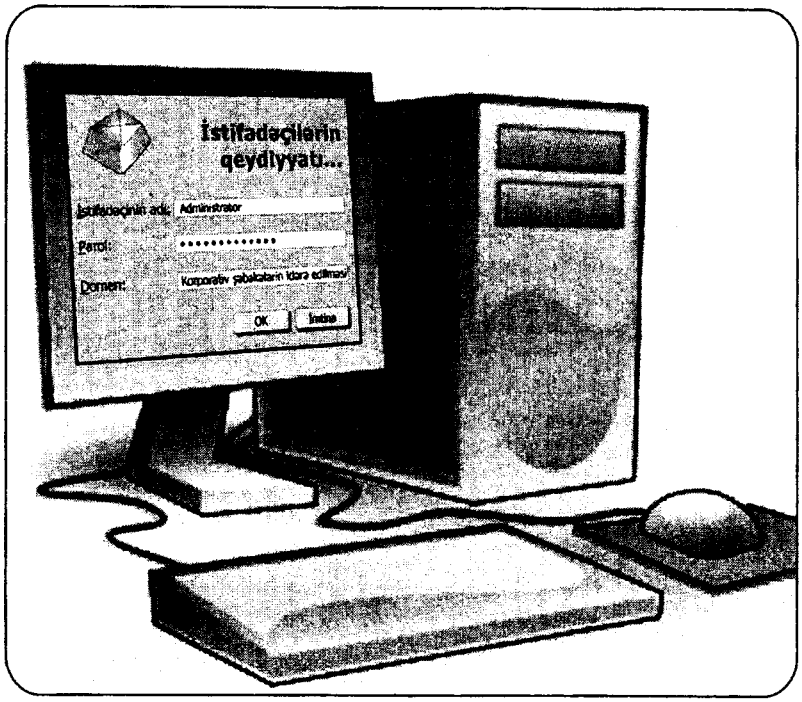
t.e.n. Elşən Rasif oğlu Rəhimov

Elmi Redaktor:

t.e.n. Yadigar Nəsib oğlu İmamverdiyev

Kitab AMEA İnformasiya Texnologiyaları İnstitutu Elmi şurasının qərarı ilə çapa məsləhət görülmüşdür (Protokol № 6; 25 iyul 2007).

MÜNDƏRİCAT


İstifadəçilərin qeydiyyatı...
İstifadəçinin adı:
Administrator
Parol:
Domen:
Kompüterlər şəbəkələrin idarə edilməsi
OK
İmtina

GİRİŞ

Giriş

Müasir dünyada ildən-ilə informasiya texnologiyalarının tətbiq sahəsinin genişləndiyi müşahidə olunur. Belə sürətli texnoloji inkişaf bizim respublikamızda da öz təzahürünü tapmışdır. Artıq informasiya texnologiyalarının geniş vüsət aldığı bir zamanda dövlət tərəfindən bu sahəyə böyük diqqət ayrılır. Qeyd etdiyimiz bu məsələni Azərbaycan dövləti tərəfindən qəbul olunan "Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2005 – 2008-ci illər üçün Dövlət Proqramı (Elektron Azərbaycan)", "Telekommunikasiya haqqında Azərbaycan Respublikasının Qanunu", "İnformasiya əldə etmək haqqında Azərbaycan Respublikasının Qanunu", "Elektron ticarət haqqında Azərbaycan Respublikasının Qanunu" və digər normativ sənədlər təsdiqləyir.

Son illər korporativ şəbəkələrin idarə edilməsi və təhlükəsizlik sistemlərinin düzgün şəkildə qurulması problemi qlobal miqyasda bütün dünyanın marağını özünə cəlb etmişdir. Məhz bu səbəbdən informasiya cəmiyyətinin inkişafına həsr olunmuş, 2003-cü ilin 10–13 dekabr tarixində Cenevrədə və 2005-ci ilin 16–18 noyabr tarixində Tunisdə keçirilən Ümumdünya Sammitlərinin materiallarında bu məsələlərə ilk sıralarda yer verilmişdir. Avropada və dünyanın bir sıra qabaqcıl ölkələrində informasiya texnologiyaları ilə bağlı külli miqdarda, müxtəlif səpkidə normativ sənədlər, qanunlar mütamadi olaraq qəbul edilməkdədir. Qanunvericiliklə yanaşı informasiya texnologiyalarının ayrı-ayrı sahələri, xüsusən də korporativ şəbəkələrdə idarəetmə və təhlükəsizlik məsələləri ilə çox ciddi şəkildə məşğul olan, habelə müvafiq standartlar təklif edən beynəlxalq standartlaşdırma təşkilatları da mövcuddur.

Artıq informasiya texnologiyalarının müxtəlif variantlarda ayrı-ayrı sahələrin aparıcı amillərindən biri olduğu danılmaz faktdır. Korporativ şəbəkədən istifadə edən istifadəçilərin sayı

çoxaldıqca korporativ şəbəkələrin sayı da durmadan artır. Müasir dövrdə bazar münasibətlərinin fundamental inkişafı sayəsində nəhəng şirkətlər, habelə təşkilatlar arasında rəqabətin dərinləşməsi korporativ şəbəkələri müasir biznes aləminin ayrılmaz bir hissəsi kimi formalaşdırır. Korporativ şəbəkələrin yaradılması və istismar edilməsi, vahid informasiya məkanının əmələ gəlməsi problemini həll edərək, həmçinin təşkilat daxili məsələlərə aid olan resurslarla təchiz olunma, xidmətlər, məhsulların istehsal olunması, təşkilatı məsələlərin həll olunması, marketinq və maliyyə hesabatlarının ardıcıl şəkildə aparılması məsələlərinin kompleks şəkildə həll olunması problemini də çözmüş olur. Digər tərəfdən korporativ şəbəkələr effektiv alət kimi vahid qəbul olunmuş idarəetmə sistemi qanunlarının və strategiyasının korporasiyaya daxil olan şirkətlərə tətbiq olunmasında böyük rol oynayır.

Korporativ şəbəkələrin tətbiqinin əsasında qloballıq, açıqlıq və əlyetənlik ideologiyasını əks etdirən dünya kompüter şəbəkəsi olan İnternet ilə inteqrasiya durur. Belə olan halda nəzərə çarpan üstünlüklərlə bərabər təhlükəsizliklə bağlı bir sıra problemlər meydana gəlir. Bu problemlərin yaranma səbəbi ilk növbədə korporativ şəbəkədə istifadə olunan proqram və aparat təminatlarının müxtəlifliyi və uyuşmaması, informasiya mübadiləsində şəbəkənin həddindən çox qovşağının iştirak etməsi, onların coğrafi baxımdan paylanmış vəziyyətdə olması, şəbəkənin bütün seqmentlərinin hamısını tam nəzarətdə saxlamağın mümkün olmaması və həmçinin korporativ şəbəkənin daxili resurslarının və ya informasiyanın xaricdən olan istifadəçilərə əlçatan olması ilə xarakterizə olunur.

Odur ki, müasir kompüter şəbəkələri əsasında korporativ şəbəkə yaradılan zaman bu infrastrukturun informasiya təhlükəsizliyinin pozulması təhlükələrindən qorumaq sualı kəskin şəkildə meydana çıxır. Məhz bu baxımdan heç təsadüfü deyil ki, son illər korporativ şəbəkənin layihələndirilməsi onun mühafizə sisteminin layihələndirilməsi ilə paralel aparılır.

Korporativ şəbəkə mürəkkəb sistem kimi qarşılıqlı əlaqədə olan bir neçə səviyyəli piramidadan ibarətdir. Korporativ şəbəkəni xarakterizə edən piramidanın aşağı səviyyəsində informasiyanın emalı və saxlanması mərkəzlərinin kompüterləri yerləşir. Onlar da şəbəkəyə məxsus olan kompüterlərin arasındakı informasiya mübadiləsinin qüsursuz olmasına cavabdehlik daşıyırlar. Şəbəkə infrastrukturunun üzərində şəbəkə əməliyyat sistemləri səviyyəsi işləyir. Bunlar da proqram təminatlarının kompüterdə müntəzəm işinin təşkil olunması və şəbəkə infrastrukturu vasitəsi ilə öz kompüterinin resurslarını ümumi istifadəyə çıxarılmasını təmin edirlər. Əməliyyat sistemlərinin üzərində müxtəlif təyinatlı proqramlar işləyirlər. Növbəti səviyyədə sistem servisləri fəaliyyət göstərir, hansılar ki, verilənlər bazasının idarəetmə sistemindən bir axtarış aləti kimi istifadə edib kompüterlərdə olan milyardlarla baytlar arasından istifadəçiyə rahat qəbul edəcəyi bir şəkildə informasiyanı təqdim edir. Verilmiş təşkilat üçün spesifik olan məsələləri həll etməkdən ötrü korporativ şəbəkənin daxili arxitekturasının ən yuxarı səviyyəsində xüsusi proqram vasitələri təqdim olunur.

Korporativ şəbəkələrin yekun məqsədi onun daxili strukturunu təşkil edən səviyyələrin ən yüksəyində tətbiqi proqramların tam şəkildə işləməsidir. Odur ki, korporativ şəbəkənin uğurlu işləməsi üçün onun digər səviyyələrinin öz funksiyalarını dəqiq yerinə yetirməsi vacibdir. Adətən kompüterlərin qarşılıqlı əlaqədə işləməsi şəbəkə infrastrukturunun əsasını təşkil edir və "korporativ şəbəkə" anlayışı da özəyini məhz buradan götürmüşdür. Digər elementlər, məsələn, səviyyələr və şəbəkə komponentləri isə sadəcə əlavə sazlama parametrləri kimi qəbul olunur. Korporativ şəbəkənin infrastrukturu bir sıra altsistemlər və elementlərdən ibarətdir. Fiziki olaraq korporativ şəbəkənin əsasını korporasiyanın lokal və qlobal şəbəkələri təşkil edir.

İstifadəçilərin informasiya resurslarına məsafədən giriş imkanının təşkili korporativ şəbəkənin mərkəzi verilənlər bazası yerləşən serverlərində realizə olunur. Məhz bu məsələ, yəni istifadəçilərin informasiya resurslarına məsafədən girişin təşkil olunması son zamanlar böyük təşkilatlar üçün vacib və strateji əhəmiyyət kəsb edir. Lakin informasiya resurslarına məsafədən giriş təşkil olunan zaman müsbət cəhətlərlə yanaşı bir sıra mənfi cəhətlər də meydana çıxır ki, bu da onların təhlükəsizliyi ilə bağlıdır. Praktiki olaraq bütün mövcud korporativ şəbəkələrin zəif nöqtələri və boşluqları mövcuddur, həm daxili və həm də xarici hücumlar üçün açıqdır. Əksər hallarda istifadəçilər bilmirlər ki, onların kompüterlərinin və ya yerləşdiyi korporativ şəbəkənin seqmentinin boşluqları mövcuddur. Bunun nəticəsi olaraq istifadəçilərin informasiya resursları təhlükə altında olur və icazəsiz istifadə oluna bilər. Adətən artıq hücum baş verəndən, sistemə virus düşəndən və ya sistem sıradan çıxarılandan sonra istifadəçilər bu boşluqlar haqqında məlumatlanırlar. İldən-ilə korporativ şəbəkədə baş verən insidentlərin sayı durmadan artmaqdadır. Bu artım öz növbəsində çox böyük maddi və mənəvi itkilərlə müşayiət olunur. Bütün yuxarıda sadalanan çatışmazlıqlar korporativ şəbəkələrin idarəetmə və mühafizə sistemlərində olan boşluqlarla izah olunur.

Bu kitabın məqsədi korporativ şəbəkələrin MS Windows Server 2003 əməliyyat sistemi əsasında idarə olunmasında və layihələndirilmə mərhələsində təhlükəsizliyinin qorunmasında mövcud problemlərin incəlikləri ilə izah olunmasından ibarətdir.

Korporativ şəbəkələrin idarə olunması dedikdə nəzarəti həyata keçirmək üçün bir sıra funksiyaları yerinə yetirmək, planlaşdırmaq, qərar vermək, tətbiq etmək, koordinasiya etmək və korporativ şəbəkəyə məxsus olan resursların monitorinqini keçirmək nəzərdə tutulur. Əgər bu sadaladığımız funksiyalara daha dərindən nəzər yetirsək onda görmək olar ki, korporativ şəbəkələrin idarə olunmasının əsasını başlanğıc şəbəkə planlaşdırılması, tezliklərin paylanması, trafikin marşrutunu təyin

olunması, kriptoqrafik açarların paylanması, konfiqurasiyanın idarə olunması, sistemin dayanıqlığı, təhlükəsizliyi, işləmə keyfiyyəti və qeydiyyat məlumatları təşkil edir. Korporativ şəbəkələrin idarə olunması üçün bir sıra hazır modellər də mövcuddur. Bunlardan FCAPS modelini göstərmək olar:

(F) Fault Management / Sapmaların idarə olunması
(C) Configuration Management / Konfiqurasiyanın idarə olunması
(A) Accounting Management / Qeydiyyatın idarə olunması
(P) Performance Management / Məhsuldarlığın idarə olunması
(S) Security Management / Təhlükəsizliyin idarə olunması

- Fault Management – şəbəkə problemlərini müəyyən edib onları aradan qaldırmaq, nasazlıqlar haqında məlumatları emal etmək, şəbəkə elementlərini test və diaqnostika etmək kimi funksiyalara cavabdehdir;
- Configuration Management – şəbəkənin aparat və proqram təminatlarının monitorinqinə və nəzarətinə cavabdehdir;
- Accounting Management – şəbəkə resurslarının prioritetlərə uyğun paylanması və istifadə olunmasına cavabdehdir;
- Performance Management – korporativ şəbəkənin real rejimdə işləməsi haqqında statistikanın hazırlanmasına, zəif yerlər və boşluqların minimallaşdırılmasına, şəbəkənin istifadəsində əmələ gələn tendensiyaların müəyyən edilməsinə və gələcək ehtiyaclar üçün resursların planlaşdırılmasına cavabdehdir;
- Security Management – icazələrə nəzarət, xarici və daxili təhlükələrdən mühafizəni təmin etmək kimi əhəmiyyətli funksiyalara cavabdehdir.

Korporativ şəbəkədə mövcud olan təhlükələrin statistik verilənlər əsasında təhlükəsizlik servislərinə görə siniflərə ayrılması və korporativ şəbəkələrin layihələndirilmə mərhələsində informasiya təhlükəsizliyinin qiymətləndirilməsi metodunun işlənib hazırlanması bu kitabın elmi yeniliyini təsdiqləyir. Kitabın praktik baxımdan əhəmiyyəti ondan ibarətdir ki, ixtiyari arxitekturaya malik korporativ şəbəkənin idarə edilməsində və informasiya təhlükəsizliyinin qorunmasında müxtəlif məqamların

konkret izahı və yeni yanaşma müfəssəl şəkildə verilmişdir.

Qarşıya qoyulmuş məqsədlə əlaqədar kitabda aşağıdakı məsələlərə baxılmışdır:

- Şəbəkə platformalarının daxili strukturunun və aparat təminatını öyrənilməsi;
- İnformasiyanın qorunması sənətinin incəliklərinin öyrənilməsi;
- Korporativ şəbəkələrdə təhlükələrin, hücumların analizi və reallaşma mexanizminin öyrənilməsi, insidentlərin toplanması, qeydiyyata alınması və emal olunması;
- Şəbəkələrdə informasiya təhlükəsizliyinin qiymətləndirilməsi üçün etibarlılıq modellərinin təhlili və seçilməsi;
- Şəbəkələrin layihələndirilmə mərhələsində informasiya təhlükəsizliyinin qiymətləndirilməsi metodunun işlənilməsi;
- Serverin proqram və aparat səviyyəsində idarə olunması.

Kitabın birinci fəslində korporativ şəbəkələrin proqram-texniki təminatı haqqında məlumat verilmişdir. Korporativ şəbəkələrin istismarı zamanı istifadə olunan və ən geniş yayılmış əməliyyat sistemləri, şəbəkə servisləri, texniki və proqram platformaları haqqında müqayisəli şəkildə izahat verilmişdir. Şəbəkə platformalarının xarakteristikaları, üstünlükləri, birindən digərinə miqrasiya və lisenziya kimi problemləri bu fəslin məzmununu təşkil edir.

İkinci fəsildə informasiyanın qorunması və məhv edilməsi adı altında korporativ şəbəkələrin qurulmasında və istismarında geniş istifadə olunan proqram vasitələrinin qorunmasının aktual məsələləri və mühafizəsinin əsas səbəbləri verilmişdir. Proqram vasitələrinin qorunmasının təmin edilməsi yollarında olan boşluqlar və çatışmazlıqlar haqqında məlumat da bu fəsildə yer almışdır.

Üçüncü fəsildə korporativ şəbəkələrin gələcəkdə idarə edilməsi üçün vacib olan korporativ şəbəkələrin layihələndirilmə mərhələsində informasiya təhlükəsizliyinin qiymətləndirilməsi

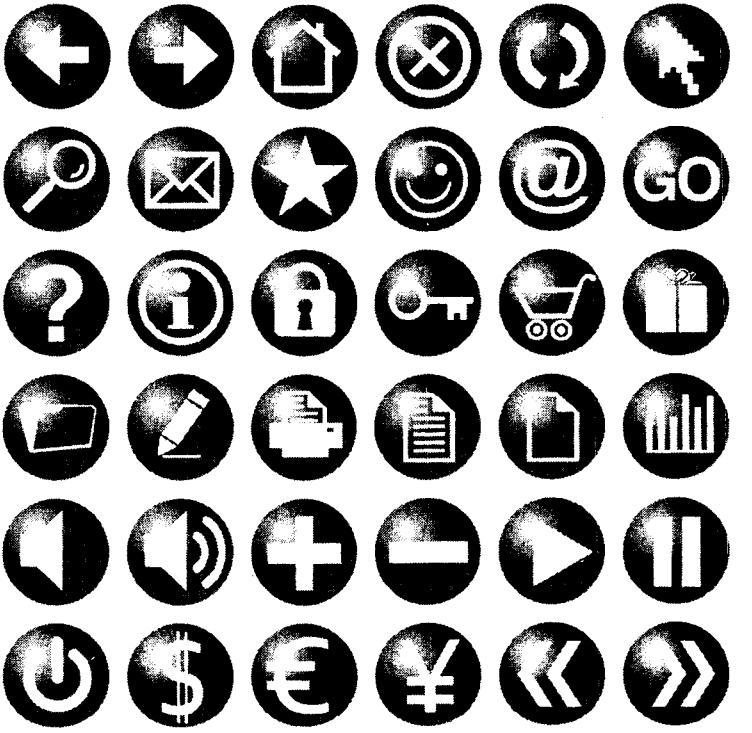
məsələsinə baxılmışdır. Burada mövcud olan təhlükələrin korporativ şəbəkələrdə reallaşma texnologiyasının müqayisəli analizi və korporativ şəbəkənin informasiya təhlükəsizliyinin qiymətləndirilməsi üçün uyğun etibarlılıq modelinin seçilməsi məsələsinə diqqət yetirilmişdir. Fəslin son iki bəndində isə layihələndirilmə mərhələsində olan korporativ şəbəkənin informasiya təhlükəsizliyinin qiymətləndirilməsi üçün metodlar işlənib hazırlanmışdır.

Dördüncü fəslin əsası korporativ şəbəkənin idarəetmə mərkəzi olan server xidmətləri, onlardan istifadə qaydaları və həmçinin şəbəkə servislərinin təşkilindən ibarətdir. Korporativ şəbəkənin idarə olunmasında danılmaz xidmətləri olan Active Directory, "sistem jurnal" və onların funksional imkanları haqqında geniş məlumat verilmişdir.

Beşinci fəsildə korporativ şəbəkənin idarəetmə sisteminin əsasını təşkil edən icazələr siyasətinin imkanları təhlil olunaraq icazələr prioritetlərə görə səviyyələrə qruplaşdırılmışdır. Proqram-aparat təminatı vasitələri ilə bərabər inzibati vasitələr də nəzərdən keçirilmişdir. Həmçinin bu fəsildə şəbəkə platformalarına xas olan bəzi təhlükəsizlik şablonlarına, korporativ şəbəkənin təhlükəsizlik siyasətinin idarə olunmasının avtomatlaşdırılmasına və şəbəkəni məsafədən idarəetmə məsələlərində olan bəzi qaranlıq məqamlara aydınlıq gətirilmişdir.

Kitabın altıncı fəslində terminal serverin fəaliyyəti hərtərəfli öyrənilmişdir. Burada terminal serverin quraşdırılması, sazlanması və işə salındıqdan sonra xidmət göstərilməsi aspektləri nəzərdən keçirilmişdir.

Nəhayət, sonuncu yeddinci fəsildə isə korporativ şəbəkələrdə qrup siyasətinin üstünlükləri, idarə olunması və tətbiqi məsələlərinə baxılmışdır. Həmçinin bu fəsildə domenlərin idarə olunması, meşələrarası etibar münasibətləri və korporativ şəbəkələrin idarəetmə mexanizmində instrumental vasitələr haqqında geniş izah verilmişdir.



FƏSİL 1

KORPORATİV ŞƏBƏKƏLƏRİN PROQRAM – TEXNİKİ TƏMİNATI

KORPORATİV ŞƏBƏKƏLƏRİN PROQRAM– TEXNİKİ TƏMİNATI

- Şəbəkələrin proqram-texniki təminatı
- MS Windows Server 2003 əməliyyat sisteminin xarakteristikalarının qiymətləndirilməsi
- MS Windows NT Serverindən keçid
- MS Windows 2000 Serverindən keçid
- DHCP Serverinin quraşdırılması
- DHCP serverinin sazlanması
- Lisenziya siyasətinə əməl olunması
- Real şəbəkənin praktik tərəfi

Fəsil 1. KORPORATİV ŞƏBƏKƏLƏRİN PROQRAM – TEXNİKİ TƏMİNATI

1.1 Şəbəkələrin proqram-texniki təminatı

Bu fəsildə korporativ şəbəkələrin idarə olunmasına dair demək olar ki, konkret misallar verilməmişdir. Lakin şəbəkə administratorunun işinin təşkil olunmasına ümumi rəylər verilir, proqram və aparat vasitələrinin tətbiqindən bəhs edilir ki, bunlarsız da şəbəkənin işi və idarə olunması çox az effektli olardı. Ona görə də bu fəsli diqqətlə oxumaq məsləhət görülür. Buradakı tövsiyələr və rəylər korporativ şəbəkələrin idarə olunmasının real təcrübəsinə əsaslanaraq verilmişdir. Ehtimal olunur ki, oxucu lazımi qədər təcrübəli fərdi kompüter (FK) istifadəçisidir, kompüterin şəbəkədəki işi ilə tanışdır və şəbəkənin işləmə prinsipi haqqında əsas biliklərə malikdir. İlkin hazırlıqdan asılı olaraq bu fəslin materialları olduqca sadə və ya olduqca çətin qəbul oluna bilər. Daha sonra şəbəkə qurğuları və proqram platforması haqqında ətraflı məlumat veriləcəkdir. Kitabda göstərilən məsələlərin əsasında qurulan şəbəkə bir neçə serverdən və onlarla kompüterdən ibarətdir. Əgər şəbəkə olduqca kiçikdirsə, onun genişləndirilməsi vacib məsələlərdən biridir. Yəni şəbəkədə edilən bütün dəyişikliklər aparılan genişlənmənin imkanları daxilində olmalıdır. Bunları nəzərə alaraq şəbəkənin inkişaf perspektivi əsasında biz ona uyğun vasitələr və administratorun iş metodunu seçirik.

Əldə lazım olan materiallar, avadanlıq və mexanizmlər, nəqliyyat vasitələri, tikinti üçün uyğun sahə, plan və layihə olmadıqda evin tikilməsi qeyri-mümkündür. Əgər hər hansı bir təşkilat özü üçün şəbəkə qurursa, onda bu kitab bu işdə elmin son nailiyyətləri əsasında şəbəkənin qurulmasında yardımçı ola bilər. Korporativ şəbəkə administratorunun vəzifəsi əvvəlcədən təyin olunmuş müddəalar əsasında qurulmuş şəbəkəni həmişə işlək vəziyyətdə saxlamaq, bəzi hallarda lazım gələrsə modernləşdirmə

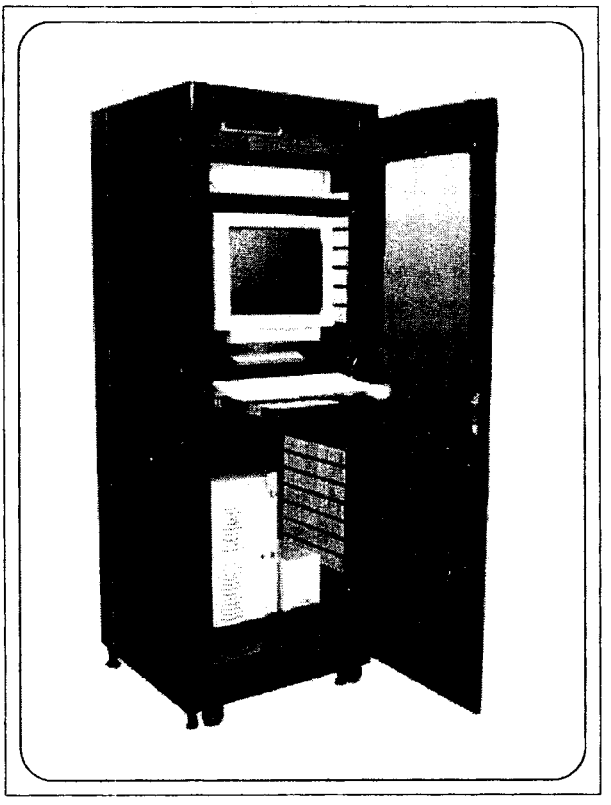
aparmaqdan və. s. ibarətdir. Bu fəsildə verilən tövsiyələr bütün hallarda şəbəkənin daim saz işləməsinə xidmət edir.

Lokal şəbəkə administratorunun iş yeri. Şəbəkənin bəzən çox böyük sahədə yerləşməsinə baxmayaraq və ona qoşulan hər hansı kompüterə daxil olmaq (avtorizasiya) lazım olduğu üçün iş yeri imkan daxilində əsas serverə yaxın olmalıdır. Bu həm də korporativ şəbəkənin administratorunu artıq gəzməkdən azad edir və təxirəsalınmaz işlərin yerinə yetirilməsində operativliyi təmin edir. Heç kimə sirr deyil ki, istər avadanlıq, istərsə də proqram təminatı nə qədər etibarlı olsa da, onların yenə də ayrı-ayrı proqramlardan asılılığı qaçılmazdır. Bu halda hətta əldə olan xüsusi məsafədən idarəetmə vasitələrinin köməyi ilə problemin həlli mümkün olmur. Ona görə də administratorun serverin yanında şəxsi iştirakı vacibdir. Odur ki, iş yeri, daha dəqiqi iş kompüteri server kompüteri ilə üst-üstə düşməlidir. Ən yüksək hazırlığa baxmayaraq heç kim səhvdən sığortalanmayıb. Serverin işi zamanı buraxılan səhv şəbəkənin uzun müddət boş dayanmasına gətirib çıxarır. Əlbəttə, serveri tamam söndürmək və ya yenidən işə salmaq mümkün olmasa da, bu işlərin görülməsinə sərf olunan vaxt minimallaşdırılmalıdır. Praktikaya əsaslanaraq demək olar ki, serverin hər 101 gündə, hər hansı ciddi və ya qeyri-ciddi səbəbdən (10-30 dəqiqə), bir dəfə dayanması, şəbəkənin işində proqram təminatının yeniləşməsi ilə əlaqədar qısa dayanmaları və ayda bir dəfədən çox olmayaraq 3-4 dəqiqə dayanması məqbul sayılır. Bu işlər yerinə yetirilərkən şəbəkə istifadəçilərinin böyük hissəsinin işi dayanır. Odur ki, administrator şəbəkənin fasiləsiz iş rejiminə daim nəzarət etməlidir.

Beləliklə, administratorun optimal iş yeri server otağıdır. Mümkün haldır ki, bu server otağına şəbəkənin digər şəbəkələrlə birləşdirən kabellər toplusu, kommutatorlar və digər şəbəkə qurğuları yerləşdirilə bilər. Adətən yeni işə başlayan

administratorlar şəbəkədə əmələ gələn hər hansı bir problemi kabellərin və ya şəbəkə qurğularının dəyişdirilməsində görürlər. Əslində şəbəkə layihələndirilən zaman onun genişləndirilməsi imkanını hökmən nəzərə almaq lazımdır, əks halda gələcəkdə şəbəkənin iflic vəziyyətə düşməsi qaçılmazdır. Məhz bu zaman şəbəkənin normal iş rejimini qaytarmaq üçün bir neçə gün tələb olunacaq, bu isə korporativ idarəetmədə qəti yol verilməzdir. Ona görə də gələcəkdə yarana biləcək problemlərin qarşısını almağa həmişə hazır olmaq lazımdır. Təbii ki, bu tip hazırlıq əlavə xərclər tələb edir. Bu isə öz növbəsində daha böyük xərclərin qarşısının alınmasına xidmət edir. Korporativ idarəetmədə, şəbəkə layihələndirilən zaman həmin ana lazım sayılmayan xərclər vaxt keçdikcə özünün vacibliyini ortaya qoyur. Şəbəkənin layihələndirmə mərhələsində yuxarıda qeyd olunan xərclər nəzərə alınmadıqda, zaman çatdıqda tələb olunan xərclər ilkin xərclərdən bir neçə dəfə çox olması ilə bərabər, həm də şəbəkənin uzun müddətə dayanması ilə nəticələnir. Server otağında bütün qurğular nizamlı və məntiqi ardıcıllıqla yerləşdirilməlidir. Bunun üçün beynəlxalq standartlardan istifadə etmək lazımdır, məsələn: ISO 2382-3:1987, ISO 2382-12:1988, ISO 9241-4:1998, ISO/IEC 2382-4:1999, ISO/IEC 9995-1:2006 və ISO 9241-400:2007. Şəbəkənin daxili strukturundan asılı olaraq server otağında yerləşən şəbəkə qurğularının birləşməsi və miqdarı müxtəlif kombinasiyada ola bilər. Həm praktikadan, həm də beynəlxalq standartlardan məlumdur ki, server müstəqil şəkildə "fasiləsiz cərəyan mənbəyi" qurğusuna qoşulmalıdır. Digər şəbəkə qurğuları isə birlikdə sayca ikinci fasiləsiz cərəyan mənbəyinə qoşulmalıdır. Bu tip qoşulma, serveri və şəbəkəni tam təhlükəsiz istismar şəraiti ilə təmin edir. Server otağında istismar təhlükəsizlik qaydalarına uyğun olaraq server və şəbəkə qurğuları xüsusi təyinatlı dolabda (şəkil 1.1) yerləşdirilir ki, bu da öz növbəsində avadanlığın qorunmasına və daha uzunmüddətli istismarına şərait yaradır. Şəbəkənin bütün kommutasiya kanalları məhz bu server dolabında

cəmlənir. Server dolabı xüsusi istilik keçirmə qabiliyyəti olan dəmirdən, şüşə qapılardan və termostatdan ibarətdir.



Şəkil 1.1 Xüsusi təyinatlı server dolabı

Termostatın server dolabındakı rolu daxili temperaturu tənzimləməkdən ibarətdir. Şüşə qapılar isə şəbəkə qurğularının indikatorlarının aydın şəkildə müşahidə etmək imkanını yaradır.

Proqram təminatı. Şəbəkə administratorunun ilkin monitorinq aparması üçün və inzibatı işləri yerinə yetirməsi üçün serverdə bir neçə proqram təminatının olması vacibdir. Bu

proqram vasitələri administratorun idarəetmədə əsas alətlərindəndir. İlk öncə əməliyyat sisteminin vacib elementlərini və imkanlarını nəzərdən keçirək. Günümüzün reallığına uyğun olaraq əksər istifadəçilərin kompüterləri MS Windows XP əməliyyat sistemi ilə təchiz olunmuşdur. Bütün şəbəkə əməliyyatlarını sərbəst şəkildə yerinə yetirmək üçün istifadəçinin kompüteri MS Windows XP əməliyyat sisteminin "Professional" versiyası ilə təchiz olunmalıdır. Əməliyyat sisteminin bu versiyası ilə şəbəkəni ixtiyari formada idarə etmək mümkündür. Əməliyyat sistemini mütəmadi olaraq prosedur qaydalarına uyğun şəkildə yeniləşdirmək (update) vacibdir. Xüsusən də Microsoft korporasiyası tərəfindən tövsiyə olunan kritik yeniləşmələr (critical updates) vaxtında yerinə yetirilərsə, əməliyyat sisteminin imkanlarını daha da genişlənər. Yeniləşmə ilk olaraq ingilis versiyası üçün buraxılır. Digər dillər üçün isə yeniləşmə bir neçə gündən sonra hazır olur. Bu problemi "istifadəçinin çoxdilli interfeysi" (MUI, Multilingual User Interface) altproqram vasitəsi ilə həll etmək mümkündür. İndi isə əlavə sistem proqram təminatları haqqında qısa məlumat verək. Administratorun şəbəkəni idarə etmək üçün istifadə etdiyi proqramların siyahısı geniş ola bilər. Bu proqramlardan bəziləri gündəlik istifadə olunur, digərləri isə ancaq lazım olduqda işlənir. Məsələn, informasiyanı bərpa etmək üçün istifadə olunan proqram vasitəsi aylarla işlənməyə bilər, lakin bu proqramın administratorun arsenalında olması vacibdir. İndi isə administratorun kompüterində və ya işçi masasında olması məsləhət olan proqramları qeyd edək.

1. Əsas ofis proqramları MS Word, MS Excel, MS Access
2. Mətn redaktoru müxtəlif sənədləri və kodları redaktə edir.

Belə redaktorların sayı bir neçə ola bilər ki, onlar da öz növbəsində lazımi və konkret vəziyyətlərdə tətbiq olunur.

3. veb-səhifə redaktoru. Əməliyyat sistemi tərkibinə daxil olan adi mətn redaktorundan və ya daha əlverişli olan xüsusi proqramdan istifadə etmək olar.

4. Fayl meneceri. Əməliyyat sisteminin imkanlarının inkişaf etməsinə baxmayaraq bütün hallarda özünü doğruldan, xüsusi olaraq MS Windows əməliyyat sistemləri üçün hazırlanan fayl meneceri "FAR"-dan istifadə olunur ki, bu da öz növbəsində müxtəlif məsələlərin həlli üçün fayllarla işləyərkən geniş və effektiv imkanlar yaradır.

5. Bir neçə xüsusi proqramlar tələb olunur ki, bu da şəbəkə skanerləridir. Onların köməyi ilə həmişə şəbəkəyə məxsus kompüterlərə və proqramlara daxil olmaq, həmçinin xidmət məsələlərini həll etmək olar.

6. Microsoft ofis proqramlarında Visual Basic for Aplication proqramlaşdırma dilinin xüsusi elementlərini nəzərə almaq lazımdır. Visual Basic for Aplication proqramlaşdırma dilini Visual Studio proqramlaşdırma paketinin daxilində tapmaq olar.

7. Məsafədən idarəetmənin vasitələri. Kitabda "Radmin" proqram vasitəsinin tətbiqinə baxılmışdır, lakin başqa proqramların tətbiq olunması mümkündür.

8. Çox hallarda korporativ şəbəkələrdə poçt serverləri və veb-serverlər tələb olunur. veb-server qabaqcıl vasitələrdən olan MS Windows Server 2003 əməliyyat sistemi əsasında işləyə bilər.

9. Poçt xidmətinin müştəriləri. Burada adi poçt xidmətindən başqa, konsol poçt xidməti göstərən vasitə də fəaliyyət göstərməlidir. Konsol poçt xidməti vasitəsi, şəbəkəni idarə etmək üçün bir sıra məsələləri avtomatlaşdırmağa imkan yaradır.

10. Əlavə proqram təminatı kimi emulyator proqramlı kompüter olması pis olmazdı. Onun köməyi ilə virtual kompüter yaratmaq olar ki, bunun vasitəsi ilə də stansiyada şəbəkənin istismarına dair

çoxlu eksperimentlər aparmaq mükün olar. Yeni proqram alətləri ilə aparılmış və müvəffəqiyyətlə başa çatmış eksperimentləri çəkinmədən şəbəkəyə tətbiq etmək olar.

11. Mühafizə sistemləri. Belə proqramların tətbiqi məcburidir.

12. Konsollu arxivator "PKZip". Bu arxivator komanda sətirində işləyərək bir neçə məsələləri avtomatik həll edir. MS Windows XP əməliyyat sistemində olan altproqramlar, "Zip" arxivlərini həm yaratmaq və həm də açmaqdan ötrü tətbiq olunurlar. Bununla yanaşı arxivlərin yayılması üçün "RAR" arxivatorundan geniş şəkildə istifadə olunur.

13. Əməliyyat sisteminin tərkibinə daxil olan administrator alətləri.

Bunlar hökmən əməliyyat sisteminin professional versiyasında olmalıdır. MS Windows XP əməliyyat sisteminin quraşdırılma diskində bir neçə əlavə vasitələr yerləşir və onların ayrı-ayrı quraşdırılması vacibdir. Göründüyü kimi indi administratorun öhdəsinə çox böyük məsuliyyət düşür.

1.2 MS Windows Server 2003 əməliyyat sisteminin xarakteristikalarının qiymətləndirilməsi

Bu fəsil Microsoft Windows Server 2003 əməliyyat sisteminin üstünlüklərinin yazılması ilə başlayır. Microsoft şirkəti proqramı hazırlayan zaman onun etibarlılığına və məhsuldarlığına, qarşılıqlı əlaqə və iqtisadi səmərəsinə çox böyük diqqət yetirmişdir.

MS Windows Server 2003 əməliyyat sisteminin üstün cəhətlərindən biridə odur ki, onu böyük təşkilatların korporativ şəbəkələrində platforma kimi istifadə etmək olar. Göstərilmiş vəsaitlərin köməyi ilə MS Windows Server 2003 əməliyyat sisteminə keçid imkanları nəzərdən keçirilmişdir. Nəticə olaraq bu əməliyyat sistemini obyektiv qiymətləndirilməsi və ona keçidin sayəsində işin operativ həllinin yüksəlməsini qeyd etmək lazımdır.

MS Windows Server 2003 əməliyyat sistemini MS Windows 2000 Server əməliyyat sistemi ilə müqayisə etdikdə, onun aşağıdakı dörd xassəyə görə üstün olduğunu aydın görürük.

1. **Etibarlılıq** – Microsoft korporasiyası tərəfindən istehsal olunan əməliyyat sistemləri arasında ən çevik və ən etibarlı olan MS Windows Server 2003 əməliyyat sisteminin müdafiə sistemi çox güclüdür. MS Windows Server 2003 əməliyyat sistemi qarşılıqlı infrastruktura malik olduğundan o informasiyanın mühafizə olunmasına tam şərait yaradır. Bu əməliyyat sisteminin etibarlılığı, hazırlığı və miqyaslılığı imkan yaradır ki, şəbəkə infrastrukturunda istifadəçilər lazım olan tələbləri yerinə yetirə bilsinlər.

2. **Məhsuldarlıq** – MS Windows Server 2003 əməliyyat sistemi korporativ şəbəkəni idarə etmək üçün sistem alətlərlə təmin olunmuşdur. Bu alətlərin köməkliyi ilə müəssisənin şəbəkə infrastrukturunun idarə olunması təmin edilir. Onlar şəbəkəni təşkilatın tələblərinə uyğun layihələndirilməsinə və istifadə olmasına şərait yaradır. Əməliyyat sistemində olan idarəetmə siyasətinin vasitələri ilə tapşırığın avtomatlaşdırılmasında, modernləşdirmə prosesinin sadələşdirilməsində şəbəkəni idarə edərək, administratora yardımçı olur. Bundan əlavə əməliyyat sistemi bir sıra tipik xərcləri azaltmağa imkan yaradır, çünki istifadəçi özü çox saylı məsələləri həll edir.

3. **Qarşılılıq** – MS Windows Server 2003 əməliyyat sistemi tətbiqi məsələlərin infrastrukturunun təşkil edilməsinə köməklik göstərir. Yəni əməkdaşlarla, müttəfiqlərlə, sistemlə və müştərilərlə yaxşı qarşılıqlı əlaqə yaradır. Ona görə də əməliyyat sistemində olan qarşılıqlı əlaqəli "Veb Server" və "Fayl Server" vasitəsilə intraşəbəkə və İnternet şəbəkəsi üçün təhlükəsiz, dinamik veb sayt yaranır. Əməliyyat sisteminin qarşılıqlı əlaqəli serverinə əlavələr etmək mümkündür və XML veb-servisin idarə olunması məsələlərinin asanlaşdırılması nəzərdə tutulmuşdur.

4. İqtisadi səmərəlilik – Microsoft şirkətinin rəqiblərinin istehsal etdiyi apaıat və proqram təminatı sistemləri, MS Windows Server 2003 əməliyyat sistemindən iqtisadi cəhətdən və infrastruktur baxımından çox geridə qalır. Buna baxmayaraq Microsoft şirkəti daim axtarışdadır və əməliyyat sistemi üçün yeni proqramlar, çevik işləyən metodlar və iqtisadi cəhətdən daha səmərəli yeni modellər yaratmaqdadır.

Etibarlılıq - MS Windows Server 2003 əməliyyat sisteminin hazırlamasında vacib məsələlərdən biri onun etibarlığını daha yüksək səviyyədə olmasıdır. Yəni MS Windows 2000 Server əməliyyat sistemini yaradarkən mövcud olan texnologiyaların üstün cəhətlərindən istifadə olunmuşdur. Məsələn, Smart kartın tutumu, Plug and Play, şəbəkə resurslarının istifadəsinin tənzimlənməsi (bandwidth throttling). Yeni texnologiya sayılan ümumdilli əvəzetmə vasitəsi "CLR-Common Language Runtime" müdafiə vasitələrini gücləndirir, şəbəkəni zərərli və ya keyfiyyətsiz proqramların təsirindən qoruyur. Bundan əlavə "Internet Information Services" (IIS) 6.0 versiyası, "açıq açarlar infrastrukturu" (PKI - Public Key Infrastructure) və "Kerberos" - MS Windows Server 2003 əməliyyat sisteminin təhlükəsizliyinin təminini daha etibarlı edir. Təhlükəsizlik baxımından korporativ şəbəkələrdə Microsoft Active Directory servisinin keyfiyyətli və operativ işini təşkil etmək üçün domenlərin kontrollerlərində olan istifadəçilərin parametrlərinin daha effektiv sinxronlaşdırılması, replekasiyası və keşlənməsi vacibdir.

Hazırlıq. MS Windows Server 2003 əməliyyat sistemi klasterlərin genişlənməsi sayəsində daimi hazırlığın saxlaması üçün böyük imkanlar yaradır.

Klasterlərin dəstəklənməsi ixtiyari təşkilat üçün mütləq və vacibdir, odur ki, onun köməkliyi ilə kritik vacib proqram əlavələrdən istifadə edilir, o cümlədən elektron ticarət üçün, ona görə ki, klasterlərin hazırlığı, miqyaslılığı və idarə olunmasını nəzərə çarpacaq dərəcədə yüksəldir. MS Windows Server 2003

əməliyyat sistemində quraşdırılan və nizamlanan klasterlər, özündən əvvəlki MS Windows əməliyyat sisteminə nisbətən nəzərə çarpacaq dərəcədə sadələşdirilmişdir. Şəbəkə vasitələri çox böyük imkanlara malik olduğundan onlar sapma zamanı (failover) boş dayanmanın qarşısını alır.

MS Windows Server 2003 əməliyyat sistemi, ölçüsü 8 bəndə qədər olan klasterləri müəyyən etmək qabiliyyətinə malikdir. Əgər bəndlərdən biri sıradan çıxarsa və ya reqlament olunmuş qaydada bərpa işlərinə dayandırılıbsa, onda həmin bənd digəri ilə dərhal əvəz olunur. Bu prosesin adı sapmalar zamanı qarşılıqlı əvəzolunma (failover) adlanır. MS Windows Server 2003 əməliyyat sistemi şəbəkədə proqram yüklənməsinin tarazlaşdırma prosedurunu (NLB), TCP protokolunun trafikini bəndlər arasında paylanmasını dəstəkləyir.

Miqyaslılıq. MS Windows Server 2003 əməliyyat sistemi simmetrik çox prosesli sistemin və klasterlərin köməkliyi vasitəsi ilə miqyaslılığı həm hündürlüyünə və həm də eninə, yəni hərtərəfləri əhatə etməklə həyata keçirir. Daxili testlər nəticəsində məlum olmuşdur ki, MS Windows 2000 Server əməliyyat sisteminə nisbətən, MS Windows Server 2003 əməliyyat sisteminin fayl sistemlərinin məhsuldarlığı 140% artıqdır. Digər komponentlərin məhsuldarlığı da nəzərə çarpacaq dərəcədə yüksəkdir, bunlardan Active Directory, Veb-Server, Terminal Server və şəbəkə xidmətlərini göstərmək olar. MS Windows Server 2003 əməliyyat sisteminin miqyaslılığı $1 \div 32$ prosessorlu sistemi əhatə edir. O həm 32 və həm də 64 bitlik sistemlərin tələblərinə cavab verir.

Təhlükəsizlik. Hal-hazırda təşkilatlar ənənəvi lokal şəbəkələrindən daha əlverişli və daha inkişaf etmiş intra və ekstra şəbəkələrə, İnternet texnologiyaları əsasında işləyən şəbəkələrə keçirlər. Nəticədə şəbəkələrin təhlükəsizliyi təmin olunur. Microsoft əməliyyat sistemləri ailəsinə daxil olan MS Windows Server 2003 əməliyyat sistemində olan sapmaları və

uyğunsuzluqları aşkar etməkdən ötrü çox dərin tədqiqatlar aparılmışdır. MS Windows Server 2003 əməliyyat sistemi təhlükəsizliyi təmin edən bir neçə vacib vasitələrlə təchiz olunmuşdur. Bu tip vacib elementlərdən biri kimi "CLR" vasitəsini göstərmək olar. Bu proqram vasitəsi proqramlaşdırma zamanı geniş yayılmış səhvlərin, sapmaların və boşluqların sayını azaltmağa imkan verir. Bundan əlavə "CLR" vasitəsi sistemin səhvsiz işləməsinə nəzarət edir və proqramın ancaq icazə verilmiş formada yerinə yetirilməsinə tam təminat verir.

Internet Information Serices 6.0. veb-serverin müdafiə olunma qabiliyyətini yüksəltməkdən ötrü başlanğıc quraşdırılma zamanı IIS 6.0 minimal rejimdə quraşdırılır (locked down). IIS 6.0-da olan mühafizə sistemlərindən şifrələmə xidməti, yaxşılaşdırılmış daydjest-autentifikasiya və sazlanmış idarəetmə hüququ ilə prosessora daxil olmaq funksiyalarını göstərmək olar. Bunlardan başqa da IIS 6.0 bir neçə yeni müdafiə vasitələrinə malikdir və onların vasitəsi ilə İnternet şəbəkəsində təhlükəsiz biznes əməliyyatları aparılır.

Məhsuldarlıq. MS Windows Server 2003 əməliyyat sisteminin ən vacib prioritetlərindən biri məhsuldarlıqdır. Onun köməkliyi ilə sistemin idarə olunmasında çox geniş imkanlara nail olmaq olar. MS Windows Server 2003 əməliyyat sisteminin axtarış interfeysi hər hansı bir məsələnin həlli yollarının axtarılmasını asanlaşdırır. "Microsoft Management Console" (MMC) və Active Directory vasitəsinin yaxşılaşdırılması məhsuldarlığı artırır və idarəetməni yüngülləşdirir. İdarəetmə üçün yeni vasitələr olan domenlərin adlarının dəyişdirilməsi, domen və meşələrin başdan-başa şəffaf idarə olunması, həmçinin "Resultant Set of Policy" (RSoP) vasitəsini qeyd etmək lazımdır. "MS Windows Management Instrumentation" (WMI) vasitəsinin komanda sətrindəki girişin genişləndirilməsi komponentləri administratora şəbəkəni idarə etməkdə çox geniş və unikal şərait

yaradır. Bunlar məhsuldarlığa xidmət edən ən vacib vasitələrdəndir.

Fayl və çap xidmətləri. Fayl resurslarının və çapın effektiv idarə olunması, istifadəçilərin ona daim girişinin olması və onların təyin olunmuş hüquqları daxilində hər hansı bir informasiya sisteminə daxil ola bilməsidir. İstifadəçilərin sayının artması istər lokal şəbəkədə, istər uzaqda yerləşən qovşaqlarda və hətta tərəf müqabili olan təşkilatlarda şəbəkə administratorunun yükünü artırır. Bu məqsədlə MS Windows Server 2003 əməliyyat sistemində yüksək məhsuldarlıqlı, funksional imkanlı, intellektual səviyyəyə malik fayl və çap xidmətləri mövcuddur.

Active Directory. Active Directory şəbəkədə olan obyekt haqqında informasiyanı saxlayır və onun məntiqi iyerarxiyasını təmin edir. Active Directory MS Windows Server 2003 əməliyyat sistemində yüksək məhsuldarlığa və miqyaslılığa malikdir. O həmçinin layihələndirmə zamanı, təşkilatın informasiya resurslarının idarə olunma məsələlərinin operativ həll olunmasını təmin edir.

Müşayiət vasitələri. MS Windows Server 2003 əməliyyat sistemi müşayiətin avtomatlaşdırılması kimi yeni vasitəyə malikdir və bunun köməkliyi ilə "Microsoft Software Update Services" (SUS) xidməti serveri sazlayan zaman avtomatik köməklik edir. Yeni "Group Policy Management Console" (GPMC) qrup siyasətli idarə etməni asanlaşdırır. Əmr edici vasitələr administratorlara işlərin çoxunu əmr edici konsoldan həll etməyə imkan yaradır. MS Windows Server 2003 əməliyyat sistemində GPMC vasitəsi ayrıca
komponent kimi realizə olunmuşdur.

MS Windows Server 2003 əməliyyat sistemində idarə etmənin vasitələrini, ehtiyat köçürmə və verilənləri yenidən bərpa edilməsi və həmçinin şəbəkənin mərkəzi bazasına qoşulmasını sadələşdirərək, etibarlılığı yüksəldir.

Terminal Services. Serverə əlavə rejimində MS Windows 2000 Terminal Services əsasında quraşdırılır. Terminal Services praktiki olaraq MS Windows əməliyyat sistemində əlavələrə və ya istifadəçi interfeysin özünə, yəni hər hansı hesablama qurğusuna, hətta Windows əməliyyat sistemi qurulması mümkün olmayan qurğulara girişini təmin edir. MS Windows Server 2003 əməliyyat sistemi verilənlərin saxlanması və ehtiyat surətinin çıxarılmasını sadələşdirərək, sistem administratoruna tələbi azaldaraq, onun işini xeyli yüngülləşdirir. Həmçinin yeni və təkmilləşdirilmiş fayl xidmətləri vasitəsi ilə verilmiş ehtiyat surət çıxarmasını təmin edən "Volume Shadow Copy" vasitəsinin işinə imkan yaradır. Bu unikal texnologiyanın üstün cəhətlərindən biri odur ki, indi istifadəçilər birbaşa öz Windows kompüterlərində faylların köhnə versiyalarını və ya silinmiş faylları "Shadow Copy Restory" vasitəsi ilə bərpa edə bilərlər. Bundan əlavə fayl və çap xidmətlərinin yeni imkanları, silinmiş sənədlərinin birgə istifadə texnologiyasını "Web-Based Distributed Authoring and Wercioning" (WebDAV) təmin edir. "Distributed File System" (DPS) və "Encrypting File System" (EFS) vasitələrinin genişlənməsi, həmçinin faylların saxlanması və təkrar istifadə olunması, bu vəsaitlərin dayanıqlılığını artırır.

Qarşılıqlı əlaqə. İstifadəçinin hər hansı bir yerdə yerləşməsindən və hər hansı bir qurğu ilə işləməsindən asılı olmayaraq MS Windows Server 2003 əməliyyat sistemi onun mərkəzi sistemlə əlaqəsini təmin edir. "Network Address Translation" (NAT) vasitəsindən istifadə etməklə MS Windows Server 2003 əməliyyat sistemi şəbəkə vasitələrinin "Internet Protocol version Point-to-Point Protocol over Ethernet" (PPoE) və "Internet Protocol Security" (IPSec) təhlükəsizlik vasitəsinin təkmilləşdirilməsinə nail olur.

Veb-servisləri XML IIS 6.0 - MS Windows Server 2003 əməliyyat sistemləri ailəsinin vacib komponentidir. Arxitektura baxımından təkmilləşdirilmiş IIS vasitəsinə proseslərin yeni

modeli, yüksəldilmiş etibarlılıq, miqyaslılıq və məhsuldarlıq daxildir. Susma prinsipinə görə IIS minimal rejimdə quraşdırılır. Bu da öz növbəsində təhlükəsizliyi artırır və şəbəkə administratoru əlavə proqram təminatların tələbinə uyğun olaraq qoşulma/ayırma əməliyyatını yerinə yetirir. Redaktə meta-bazasının XML xidmətinə köməyi nəticəsində idarə etmənin imkanları genişlənir.

Texniki standartlra əsasən əməkdaşlar hər hansı nöqtədən və hər hansı qurğudan şəbəkəyə qoşulma imkanına malik olmalıdırlar. Tərəfdaşlardan və təchizatçılardan tələb olunur ki, əsas resurslar vasitəsi ilə effektli qarşılıqlı əlaqə qursunlar. Təkmilləşdirilmiş və yeni şəbəkə vasitələri MS Windows Server 2003 əməliyyat sisteminin şəbəkə infrastrukturunda universallığı, etibarlılığı və təhlükəsizliyi yüksəldir.

Enterpise xidməti UDDI. MS Windows Server 2003 əməliyyat sistemində veb-serververlər XML üçün domen və dayanıqlıqlı infrastruktur yaratmaqdan ötrü "Enterpise UDDI" xidmətinə qoşulur. Bu standartlar şirkətlərə intra və ya ekstra şəbəkələrində olan daxili şəxsi servislərində UDDI xidmətindən istifadə etməyə imkan verir. Korporativ şəbəkə administratoru öz şəbəkəsini həm idarə edər və həm də proqram resurslarını kataloqlaşdıra bilər. "Enterpise UDDI" xidməti, daha intellektual və etibarlı əlavələri yaratmağa və istifadə etməyə imkan verir.

MS Windows Media Services. MS Windows Server 2003 əməliyyat sistemi media sellərinin ötürülmə xidmətini çox yüksək səviyyədə özündə birləşdirir. Bu xidmət MS Windows Media platformasının versiyalarının bir hissəsi olaraq, həmçinin yeni versiyalar olan MS Windows Media player, MS Windows Media Encoder, Audio/video kodekləri və "MS Windows Media Software Development Kit" özündə birləşdirir. Daxili təchizat NET və XML xidmətləri MS Windows Server 2003 əməliyyat sistemini ideal platformaya çevirir. "Microsoft. Net" əsasında yaradılmış veb-servislər, XML xidmətinin orada işləməsi,

yerləşdirilməsi və yayılması MS Windows Server 2003 əməliyyat sistemində qarşılıqlı işi təmin edir. XML veb-servisləri istifadə etdikdə, proqramların təhlükəsiz inteqrasiya səviyyəsi təmin olunur: diskret əlavələr – NET və XML xidmətləri qarşılıqlı əlaqə yaradaraq çevik və etibarlı yaratmanı, açılmanı, istismarı və təhlükəsiz istifadəni təmin edir. Microsoft platforması istifadəçilər üçün, XML xidməti və serverlərdə yeniliklər yaratmaqdan ötrü dəst alətlərlə təchiz olunmuşdur. XML veb-servisləri təkrar istifadə olunma komponentinə malikdir ki, bu da sənaye standartları əsasında qurulmuşdur. XML veb-servisləri başqa əlavələrə onların necə yaradılmasından, hansı əməliyyat sistemində istifadəsindən və ora giriş üçün lazım olan qurğudan asılı olmayaraq onlara müraciət edə bilər. XML veb-servislərinin köməkliyi ilə istehsalçılar həm təşkilat daxilində və həm də korporativ şəbəkədən kənarda, istifadəçi və tərəfdaşlar arasında, əlavə proqram vasitələrinin qarşılıqlı işini yarada bilərlər. Təşkilat qarşılıqlı federativ səviyyədə və daha effektli servislərdə "biznes-biznes" və "biznes-alıcı" gəlirini nəzərə çarpacaq dərəcədə artırmaq qabiliyyətinə malikdir.

İqtisadi səmərə. MS Windows Server 2003 əməliyyat sistemi yüksək etibarlılıq, xərclərin idarə olması, reqlament üzrə boş dayanmaları və təmir işlərinə sərf olunan vaxtın qısaldılması üçün geniş imkanlar yaradır. Cari tələbatdan asılı olaraq MS Windows Server 2003 əməliyyat sistemi çevik və hərtərəfli miqyas üzrə genişlənir. MS Windows Server 2003 əməliyyat sistemində idarə olunma və nizamlanma alətləri onun açılmasını və idarə olunmasını sadələşdirir. MS Windows Server 2003 əməliyyat sistemində mövcud proqramlar və müstəqil istehsalçıların proqram məhsulları ilə birgə işləməsi, təşkilatın informasiya infrastrukturuna xərclədiyi vəsaitin düzgün istiqamətə yönəldilməsini sübut edir.

1.3 MS Windows NT Serverindən keçid

Aşağıda MS Windows NT Server 4.0 əməliyyat sistemindən yeni əməliyyat sisteminə keçdikdə yaranan əsas imkanlar və irəliləyişlər göstərilmişdir. Bu məsələlərə təşkilatların və istifadəçilərin diqqət yetirməsi məsləhətdir.

Active Directory. Microsoft Active Directory xidmət kataloqu mürəkkəb şəbəkə kataloqlarında idarəetməni sadələşdirir və hətta onun şəbəkələrdə resurslarının axtarılmasını asanlaşdırır. Bu başlanğıcda İnternet standartları əsasında qurulmuş miqyaslı xidmət, MS Windows Server 2003 əməliyyat sistemi səviyyəsində qarşılıqlı əlaqə yaradır. MS Windows Server 2003 əməliyyat sisteminin Standart Edition; Enterprise Edition; və Datacentre Edition versiyalarında, Active Directory xidməti ilə işləməyi sadələşdirməkdən ötrü bir çox üstünlüklərə və yeni imkanlara: qarşılıqlı əlaqə arasındakı etibarlı əlaqə; domenlərin adlarının dəyişdirilməsi imkanı; atributların deaktivizasiyası; onların dəyişdirilməsi və təyin edilməsi üçün sxemlər sinfinə malikdir.

Qrup siyasəti: Group Policy Management Console. Administratorlar kompüter istifadəçiləri üçün parametrlərin təyinində və digər məsələlərdə qrup şəklində siyasət yeridə bilərlər. Qrup siyasətli lokal şəbəkələrdən fərqli olaraq o Active Directory xidmətində olan təşkilati bölmələrdə və domenlərdə bütün bəndlərin qaydalarını təyin edir. Qrup siyasəti vasitəsi ilə idarəetmə, sistemin modernləşdirilməsi, əlavə proqram təminatlarının quraşdırılması, istifadəçilərin problemlərinin idarə olunması, həmçinin işçi stansiyaların bloklaşdırılması bir qədər asanlaşmışdır. MS Windows Server 2003 əməliyyat sisteminin əlavə komponenti olan "add-in" quraşdırılması tələb olunan zaman, GPMC qrup siyasətinin idarə olunmasında yeni karkas təklif edir.

Serverin məhsuldarlığı. MS Windows Server 2003 əməliyyat sisteminin daxili testləri göstərir ki, fayl-serverin və veb-serverin məhsuldarlığı MS Windows NT Server 4.0 əməliyyat

sisteminə nisbətən iki dəfə artıq olur, şəbəkə və kompüter xassələrindən asılı olaraq konkret şəraitdə məhsuldarlığın yüksəlmə dərəcəsi bir-birindən fərqli olur. Buna baxmayaraq Microsoft korporasiyası əmin edir ki, MS Windows Server 2003 əməliyyat sisteminin sayəsində yüksək məhsuldarlığa və şəbəkəyə aid bütün məsələlərinin həllinə tez bir zaman kəsiyində nail olmaq olar.

Volume Shadow Copy Restore. "Volume Shadow Copy" xidmətinin bir hissəsi olaraq, administratorlara işi dayandırmadan vacib faylların surətlərinin çıxarılmasına və sonra onların bərpa olmasına və ya arxivləşdirilməsinə imkan yaradır. İstifadəçilər öz sənədlərini arxivl əşdirilmiş formada serverdə görünməz şəkildə saxlamaqla ala bilərlər.

Internet Information Services 6.0 və Microsoft .NET Framework. "IIS 6.0" çox dəyərli veb-server olaraq, XML vasitəsinin veb-əlavəsini və veb-servesi dəstəkləyir. Yeni arxitekturaya malik yaradılmış proseslər modeli veb-saytın və əlavələrin etibarlılığını sapmalara qarşı davamlılığını artırır. İndi IIS 6.0, əməliyyat sisteminin daxilində ayrı-ayrı veb-əlavələrin və ya daxildə bir neçə saytın öz başına prosesini sistem proqramların seli ilə izolə edə bilər. Bu əlavə proqram vasitələrinin imkanlarını və məhsuldarlığını yüksəldərək, nəticədə serverlərin yaddaşlarında böyük fazalar yaradır ki, bu da aparat vasitələrinə tələbi azaldır. Əlavə proqram təminatlarının sərbəst selləri server daxilində əlavə proqramlara və saytlara imkan vermir ki, veb-servislər XML vasitəsini və ya digər əlavələri bərabər şəkildə paylasın. IIS xidməti veb-əlavələrdə yaranan sapmaları müəyyən etmək və onları bərpa etmək üçün monitorinq vasitəsinə malikdir. Bərpa olunduqdan sonra onun baş vermə səbəbini aydınlaşdırmaqdan ötrü Microsoft ASP .Net, MS Windows Server 2003 əməliyyat sistemində yeni proseslər modeli kimi IIS vasitəsini istifadə edilir. Əlavə proqram üçün hal hazırda istifadə olunan IIS 5.0 və 6.0-cı versiyalar sapmalara nəzarəti gücləndirir

və bunun üçün əlavə modifikasiya tələb olunmur ki, bu da böyük əhəmiyyət kəsb edir. "Microsoft .Net Framework" proqramlaşdırma modeli ilə stabil platformada veb-əlavələr və veb-servislərin işini yerinə yetirmək mümkündür. Çoxdilli standartlar əsasında yaradılmış bu vasitə, keçmiş əlavə proqramlarla işlədiyi kimi növbəti yaranacaq servislərlə də qarşılıqlı işləyir, həm də problemlərin operativ həll olması və İnternet miqyaslı proqram təminatlarının çevik işləməsini təmin edir. Mövcud əlavə proqram təminatı olan veb-servislər vasitəsi ilə XML xidmətini çox asanlıqla yaratmaq olar. Unix əməliyyat sistemində isə qarşılıqlı işi yaratmaq üçün tətbiq etmək mümkündür. "Terminal Services" vasitəsi ilə MS Windows əməliyyat sisteminin əlavə proqram təminatlarına və ya MS Windows əməliyyat sisteminin özünün istifadəçi interfeysinə hər hansı hesablama qurğusuna, hətta orada MS Windows əməliyyat sisteminin işləməsi mümkün deyilsə belə, girişi təmin edir. İstifadəçi "Terminal Services" vasitəsi ilə əlavə proqramlarla işlədikdə, yalnız klaviatura və monitor vasitəsi ilə informasiya mübadiləsi aparır və mərkəzi serverdə bütün lazımi hesabatlar həyata keçirilir. Əməliyyat sistemində istifadəçi yalnız özünün apardığı əməliyyatı görür və digər istifadəçilərin apardığı seanslardan asılı olmur.

Remote Desktor for Administration. "MS Windows 2000 Terminal Services" əsasında inşa edilərək məsafədən idarəetmə rejimində işləyir. Bundan əlavə "MS Windows 2000 Terminal Services" tutduğu iki virtual seans rejimində administrator serverinin real konsoluna məsafədən qoşula bilər. "Terminal Services" vasitəsi təşkilatın miqyasına uyğun olaraq orada proqramın genişləndirilməsinə imkan verir. MS Windows Server 2003 əməliyyat sisteminin imkanlarına aid olan 8 bəndə qədər klasterlər "Enterprise Edition" və "Datacenter Edition" versiyalarında, elektron ünvan sistemlərində, həmçinin fayl serverlərdə və çap serverlərin yüksək hazırlığında kritik vacib

proqram əlavələrinin edilməsində miqyaslılığını təmin edir. Klasterləşdirmə bir neçə server və bəndlər arasında daimi əlaqə yolu ilə həyata keçir. Klasterin bəndlərində sapmalar zamanı və ya reqlament üzrə təmir işləri aparılan zaman giriş mümkün olmadığı anda digər klasterlərlə əvəz olunur. İstifadəçilər şübhə etmədən sıradan çıxmış bəndlə işi davam etdirir və o heç bilmir ki, ona başqa kompüter vasitəsi ilə servis göstərilir. MS Windows Server 2003 əməliyyat sisteminin " Enterprise Edition" və " Datacenter Edition" versiyaları səkkiz bəndə qədər klasterləri dəstəkləyirlər.

PKI vasitəsinin dəstəklənməsi. PKI vasitəsinin qarşılıqlı iş zamanı dəstəklənməsi üçün istifadə olunan Kerberos vasitəsi, Certeficate Services və idarəetmə alətlərinin sertifikatı imkan verir ki, təşkilat özünün açıq açarlar (PKI - Publis Key Infrasturukture) infrastrukturunu yaratsın. "PKI" vasitəsinin tətbiqi sayəsinə korporativ şəbəkənin administratorları beynəlxalq standartlar əsasında texnologiyanı, istifadəçilərin autentifikasiyasını, "Secure Sockets Layer" və "Transport Layer Security" elektron portunun mühafizəsini, rəqəmli imza və protokol üzrə müdafiə olunan birləşmələri (IPSec) yerinə yetirə bilərlər. Administratorlar "Certeficate Services" vasitəsi ilə mərkəzə sertifikat girişini həm yaradar və həm də X.509 v3 sertifikatını idarə edə bilərlər (Certefication authorities). Bu o deməkdir ki, təşkilatlar istifadəçilərin autentifikasiya xidmətindən asılı olmayacaqlar və onlar öz növbəsində təşkilatın açıq açarlar infrastrukturu ilə qarşılıqlı əlaqədə ola bilər. Kerberos vasitəsi etibarlı standart autentifikasiya şəbəkə protokolu olaraq, onun köməkliyi ilə operativ proseslər parlamentlərini birdəfəlik sistemə daxil edərək istifadəçilərin təşkilatın resurslarına və başqa vasitələrə girişini dəstəkləyir. Kerberos vasitəsinin dəstəklənməsi digər üstünlüklərlə də xarakterizə olunur. Buna misal olaraq qarşılıqlı autentifikasiyanı, yəni istifadəçi və serverin bir-birini nümayəndələrə görə autentifikasiya etməsini göstərmək olar.

Komanda sətrindən idarəetmə. MS Windows Server 2003 əməliyyat sistemi genişləndirilmiş komanda sətri infrastrukturuna malikdir və bunun vasitəsi ilə də başlıca idarəetmə məsələlərini, qrafik interfeysi tətbiq etmədən həll etməyə imkan yaradır. İnformasiya saxlanılan yerə girişi, geniş imkana malik "MS Windows Management Instrumentation" (WMI) vasitəsi tərəfindən həyata keçirilir. Komanda sətirli "WMI" vasitəsi (WMIC), sadə interfeys komanda sətrinin hesabına komanda prosessoru (Shell), sistem proqramların və ssenarilərin köməyi ilə asanlıqla genişləndirilir və ya digər proqram əlavələrinin idarə olunmasında qarşılıqlı əlaqələr yaradır. MS Windows Server 2003 əməliyyat sisteminin komanda sətrinin imkanları daxilində hazır ssenarilərdən istifadə etdikdə, uyğun digər yüksək qiymətə malik əməliyyat sistemlərinin qüvvətli vasitələri ilə rəqabət aparır. Unix və Linux sistemlərini komanda sətri vasitəsi ilə idarə etməyə adət etmiş administratorlar bunu MS Windows Server 2003 əməliyyat sistemində də istifadə edə bilərlər.

İntellektual fayl xidmətləri: *Encrypting File System, Distributed File System* və *Fill Replication service*. "EFS" fayl sistemi istifadəçiyə imkan verir ki, fiziki olaraq bu fayla girmək imkanı əldə edən, lakin icazəsi olmayan bu şəxslərdən faylı qorumaq üçün şifrələmə/deşifrələmə aparsın. Şəffaf şifrləmə: istifadəçi şifrlənmiş fayllarla və kataloqlarla adi qaydada işləyir. Əgər istifadəçi "EFS" sisteminə aid şəxsdirsə, onun faylı və kataloqu şifrlənibsə, onda təkrar müraciətdə sistem faylı avtomatik olaraq deşifrələyir. " DFS" sistemi şəbəkədə disk resurslarından istifadə edərək birgə idarə etməni sadələşdirir. Korporativ şəbəkənin administratorları tərəfindən istifadəçilərin şəbəkədə iş prosesini asanlaşdırmaq üçün şəbəkə qurğularına məntiqi adlar verməsi məqsədə uyğundur. MS Windows NT Server 4.0 əməliyyatlar sisteminin kataloq replikasiya vəsaitlərinə nisbətən "FRS" bir addım öndədir. Belə ki, "FRS" verilmiş

kataloqla, seçilmiş serverlər arasındakı çox tərəfli (multimaster) replikasiya fayllarını dəstəkləyir. Bundan əlavə "FRS" fayl sistemi, "DFS" fayl sistemi üçün o zaman istifadə olunur ki, verilmiş replika ilə seçilmiş server arasında sinxronluğun saxlanılmasını və həmçinin Active Directory vasitəsi üçün informasiyanın avtomatik sinxronluğu ilə domen nəzarətçiləri arasında əlaqə yaratsın.

1.4 MS Windows 2000 Serverindən keçid

MS Windows Server 2003 əməliyyat sistemində əlavə proqram təminatları olan XML veb-servislərinin yeni layihələri və təkmilləşdirilmiş bu əlavə proqramların qarşılıqlı əlaqəli işi nəticəsində prosesin effektivliyi yüksəlir. MS Windows 2000 Server-dən yeni əməliyyat sisteminə keçməyi planlaşdıran təşkilatlar aşağıdakı imkanlara və yeniliklərə diqqət yetirməlidirlər.

Active Directory vasitəsində təkmilləşmələr. Active Directory mürəkkəb şəbəkə kataloqlarında və hətta ən böyük şəbəkələrdə resurs axtarışında idarəetməni sadələşdirir. Bu xidmət böyük miqyasa malik təşkilatlarda İnternet texnologiyalarının standartları əsasında qurulmuşdur və MS Windows Server 2003 əməliyyat sistemin səviyyəsində "Standard Edition", "Enterprise Edition" və "Datacenter Edition" versiyaları ilə tam inteqrasiya olunmuşdur. MS Windows Server 2003 əməliyyat sistemi Active Directory xidməti ilə işləmək üçün bir sıra yeni xidmətlər təklif edir. Bu yeni imkanlara misal olaraq meşələrarası etibar münasibətlərini, domenlərin adlarının dəyişdirilməsini, atributların deaktivizasiyasını və sxem siniflərinin dəyişməsini təyin etməyə imkan verən vasitələri göstərmək olar.

Group Policy Management Console – qrup siyasəti vasitəsidir ki, onun köməkliyi ilə administrator istifadəçi və kompüterin işinə icazə verə bilər. Qrup siyasətinin lokal siyasətdən fərqi ondan ibarətdir ki, o bütün bəndlərin qaydalarını

Active Directory xidmətində domen və təşkilati hissələrini təyin edir. Şəbəkəni qrup siyasəti əsasında idarəetmə, sistemin modernləşdirilməsi, proqram əlavələrinin quraşdırılması, istifadəçilərin profillərini və işçi stansiyalarının bloklaşdırılmasını asanlaşdırır. Quraşdırılması planlaşdırılan MS Windows Server 2003 əməliyyat sisteminin komponenti (add-in) GPMC qrup siyasətinin idarə edilməsində yeni modelidir. GPMC qrup siyasətinin tətbiqini sadələşdirir.

"Resultant Set of Policy" (RSoP) – "Microsoft Management Console" (MMC) təchizat (snap–in) dəsti şəklində təqdim olunur və o adminstratorlara bu dəsti siyasət qaydaları ilə iki rejimdə təhlil etməyə şərait yaradır: qeyd etmə rejimi və planlaşdırma rejimi. Qeyd etmə rejimində administratorlar təyin olunmuş obyektə siyasət qaydalarının tətbiqinin nəticəsinə baxa bilərlər. Planlaşdırılma rejimini isə qrup siyasətində uyğun dəyişikliklər aparmadan, təyin olunmuş obyektə tətbiq olunan siyasətin dəyişdirilməsi nəticəsində nə baş verəcəyini öyrənməyə imkan verir.

Microsoft .Net Framework. "Microsoft .Net Framework" proqramlaşdırma modeli proqramlar ilə qarşılıqlı əlaqədə olaraq, veb-əlavələrin quraşdırılması, inkişaf etdirilməsini təmin edir.

Bundan əlavə olaraq həm şəbəkə üzrə və həm də standart protokol üzrə XML, veb-servisləri öz imkanı daxilində proqram girişinə malik olan "SOAP" və "HTTP" xidmətləri üçün istifadə edir. "Microsoft .Net Framework" əvvəlki əlavə sistem proqram təminatlarının qarşılıqlı əlaqələrinin standartları əsasında yaradılaraq yüksək məhsuldarlığı ilə problemlərin aradan götürülməsi və İnternet miqyasında əlavə proqram təminatı işinin operativ həll olmasını təmin edir. Proqram təminatçıları tərəfindən "Microsoft .Net Framework" xidməti MS Windows Server 2003 əməliyyat sistemi üçün elə hazırlanmışdır ki, sistem daxilində iş zamanı infrastrukturun kodunu yazmaq lazım gəlmir çünki, "Microsoft .Net Framework" bu vəzifəni öz üzərinə götürərək

qarşılıqlı idarəetməni, proqramların sadələşdirməsini və həcmini yüksəldir.

Klasterlər (8 bəndə qədər). Bu xidmət yalnız MS Windows Server 2003 əməliyyat sisteminin "Enterprise Edition" və "Datacenter Edition" versiyalarına aid olub kritik proqram əlavələrini, bunlardan verilənlər bazasını, elektron poçt sistemlərini, həmçinin fayl-serverləri və çap-serverlərinin yüksək hazırlığını və miqyaslılığını təmin edir. Klasterləşdirmə bir neçə serverlər və ya bəndlər arasında daimi əlaqə vasitəsi ilə həyata keçirilir. Sapmalar nəticəsində əgər klasterlərin bəndlərindən hər hansı birinə giriş mümkün olmayırsa dərhal onu digəri əvəz edir.

Emergency Management Services. "Başsız server" (headless server) vasitəsi ilə administrator serveri monitorsuz və video qurğusuz işini planlaşdıraraq, idarə edir. "Emergency Management Services" - bu yeni bir vasitə olaraq administratora uzaqdan idarəetməyə və bərpa etməyə şərait yaradır. Hətta server başqa standart mexanizmlərin və uzaqdan idarə etmənin alətlərinin köməyi ilə şəbəkəyə qoşulması mümkün olmadığı halda belə, uzaqdan idarəetməni təmin edir.

1.5 DHCP serverinin quraşdırılması

Lokal şəbəkələrin quraşdırılmasında əsasən şəbəkə protokolları qrupu tətbiq olunur. Bu IP protokollar İnternet şəbəkəsi yaradılan zaman onunla bərabər ixtira olunub, ona görə də onların adı indiyə qədər qorunub saxlanılaraq – "Internet Protocols" adlanır. Şəbəkə texnologiyalarının inkişafı ilə əlaqədar olaraq bu protokolları miqyasından asılı olmayaraq yaradılan bütün şəbəkələrə birgə tətbiq olunmasına gətirib çıxardı. Lokal şəbəkədə IP-texnologiyaların genişlənməsinə qədər tətbiq olunan protokollar indi demək olar ki, rast gəlinmir, yalnız kiçik bir ranqlı və ya sosial təyinatlı şəbəkələrdən başqa, hansı ki, bu kitabda onlara baxılmayıb. Bütün bunlara baxmayaraq şəbəkələrdə IP protokolu tətbiq olunur. Tanıtmanı və identifikasiyanı müvəffəqiyyətlə

yerinə yetirmək üçün şəbəkədə olan hər bir kompüterin özünün unikal IP ünvanı olması vacibdir. Unikal IP ünvanı olması şəbəkədə fasiləsiz işin təmin olunmasının əsasını təşkil edir. IP ünvanları sayına məhdudiyyət qoyulmur. Bu həm lokal şəbəkələrə və həm də İnternet şəbəkələrinə aiddir. Şəbəkələrdə işləyən bütün kompüterləri unikal ünvanla təmin etməkdən ötrü şəbəkəyə giriş zamanı dinamik mənimsəmə tətbiq olunur. Bu texnologiya daha çox sayda kompüterin unikal ünvanla təmin olunmasına imkan verir. Adətən korporativ şəbəkələrdə bütün kompüterlərin eyni zamanda ixtiyari kombinasiyada işləməsi nəzərdə tutulur. Bununla əlaqədar şəbəkəyə ünvanların dinamik üsulla tətbiq olunmasında səmərə bir qədər azalır. Buna baxmayaraq o öz üstünlüyünü saxlayır belə ki, şəbəkədə olan hər bir kompüterin unikal ünvanına nəzarət etmək administratordan tələb olunmur. Bu nəzarəti server əməliyyat sistemi yerinə yetirir. Əfsuslar olsun ki, IP ünvanlarının seçilməsi üsulu həmişə tətbiq olunmur. Bunun üzərində çox dayanmayacağıq, lakin onu qeyd etmək lazımdır ki, onun tətbiqində şəbəkənin işçi stansiyalarında bir neçə məhdudiyyətlər yaranır. Ona görə də bəzi ünvanlar dinamik, digərləri isə statik şəkildə verilir. Bu ünvanların unikallığına diqqət yetirilməlidir. Aparılan "hesabatlarda" çaşmamaq üçün əvvəlcədən qaydalar təyin edilməlidir ki, şəbəkədə İP-ünvanlarının paylaşdırılması tam şəffav olsun. Hal-hazırda bu əməliyyat edilməyibsə və ya şəbəkədə kompüterlərin sayı bir o qədər çox deyilsə, əvvəlcədən müəyyən olunmuş texnoloji tələblərə əsasən bu iş vaxtında yerinə yetirilməlidir.

İlk öncə şəbəkənin özündə IP ünvanlarının seçilməsinə diqqət yetirilməlidir. Şəbəkə üçün MS Windows 2000 Server və MS Windows Server 2003 əməliyyat sistemi ilə işləyən serverlərdə susma prinsipinə görə IP ünvan "192.168.0.0" və şəbəkə altı maska "255.255.255.0" təklif olunur. Şəbəkənin baş serveri üçün isə "192.168.0.1" IP ünvanı təklif olunur. Bu bütün

qapalı sadə şəbəkələr üçün optimal versiya kimi əməliyyat sistemləri tərəfindən dəstəklənir.

Əgər şəbəkənin genişləndirilməsi və başqa lokal şəbəkələrlə qarşılıqlı işini təmin etmək nəzərdə tutulubsa (məsələn, marşrutizatorların tətbiqi), bu vaxt qarşıya bir neçə problemlər çıxır və onların aradan qaldırılması olduqca böyük zəhmət tələb edir. Misal üçün belə bir problemi növbəti situasiyada göstərmək olar. Tutaq ki, başqa lokal şəbəkəyə qoşulmaq lazımdır. Bu lokal şəbəkənin serveri "192.168.0.20" ünvanına malikdir. Belə bir ünvan işçi stansiyalardan biri üçün nəzərdə tutulub. Uyğun olaraq DHCP-serveri işçi stansiyası üçün bu ünvanı verir və onun unikallığını güdür. Belə olan halda, digər şəbəkədə elə kompüter tapmaq lazımdır ki, onun ünvanı şəbəkədə olan ünvanlardan birinə uyğun gəlsin. Lakin bu halda serverə qoşulmaq müvəffəqiyyət gətirməyəcək. Çünki, IP ünvan təkrar olunduğundan server bu formada qoşulmağa icazə verməyəcək. Odur ki, şəbəkədə olan hər hansı bir kompüterdə xarici serveri təyin etmək mümkün olmur. Əlbəttə bu problemin həlli vardır, lakin bu böyük zəhmət tələb edir. Əgər şəbəkədə ayrı-ayrı ünvanlar vardırsa onda bu məsələlərin hamısı çox asan həll olunur. Praktikadan məlum olduğu kimi IP ünvanının üçüncü blokunda təşkilat özünə məxsus bir rəqəm təyin edə bilər. Məsələn əgər bu rəqəm 25-dirsə onda IP ünvan: "192.168.25.0" olacaqdır. IP ünvanın Birinci iki blokunun rəqəmlərini olduğu kimi saxlamaq gələcəkdə şəbəkəni genişləndirən zaman heç bir problemin meydana çıxmayacağına təminat verir. Digər tərəfdən qadağanın səbəbi ona görədir ki, bütün mümkün ünvanlar tətbiq olunmaq üçün oblastlara bölünür. Bunların bir hissəsi böyük olmayan şəbəkələr üçün, digərləri İnternet üçün, üçüncüləri korporativ şəbəkələr üçün, dördüncülər isə eksperimental şəbəkələr üçün tətbiq olunur. Əgər hər hansı bir şəbəkə özünə ünvan mənimsəyirsə, onun digər şəbəkə qrupuna aid olması təhlükəli hal sayılmır və bu zaman heç bir hadisə baş verə bilməz.

Lakin başqa şəbəkələrlə təmasda problemlərin yaranması mümkündür. Ona görə də yaxşı olar ki, qəbul olunmuş qaydalara əməl edərək şəbəkənin IP ünvanını "192.168.25.0" ilə təyin edilsin. Əg ər bir neçə şəbəkənin yaradılmasından və onlar arasında qarşılıqlı əlaqədən söhbət gedirsə onda dərhal IP ünvanların bölüşdürülməsi üçün razılığa gəlmək lazımdır. Bu yolla ehtimal olunan xarici problemlərdən özünü qoruyaraq, daxili ünvanların bölüşdürülməsinə başlamaq olar. Müxtəlif məqsədlər üçün istifadə olunan ünvanların diapazonlarını təyin etmək olduqca vacibdir. Şəbəkə üçün nəzərdə tutulan ünvanların neçə bölüşdürülməsi onun iş qabiliyyətinə təsir etmir. Əgər şəbəkələr əvvəlcədən müəyyən olunmuş qaydalar əsasında təşkil olunmuşsa o zaman onları idarə etmək çox asan olur. Şəbəkədə mümkün olan IP ünvanlar fəzasının diapazonlarının bölüşdürülməsi üçün cədvəl 1.1-də variantlar təklif olunmuşdur. Verilmiş şəbəkədə ünvanların bu cür diapazonlara bölüşdürülməsi zamanı 170 kompüterin işləməsi mümkündür. Bunlardan 49-u qeyd olunmuş ünvanları özündə saxlayır, 121 isə ünvanları avtomatik ala bilir. Hal-hazırda verilmiş şəbəkədə bu sayda işçi stansiyalar yoxdur. Serverlər bu siyahıya daxil deyillər. Amma onların inkişafı üçün bəs qədər imkanlar vardır. Lazım gəldikdə paylaşdırma qaydalarını bir qədər dəyişmək olar. Əgər şəbəkədə konkret inkişaf planı yoxdursa onda paylaşdırma qaydalarını dərhal tətbiq etmək məqsədə uyğundur.

Cədvəl 1.1

Şəbəkədə ünvanlar fəzasının diapazonları

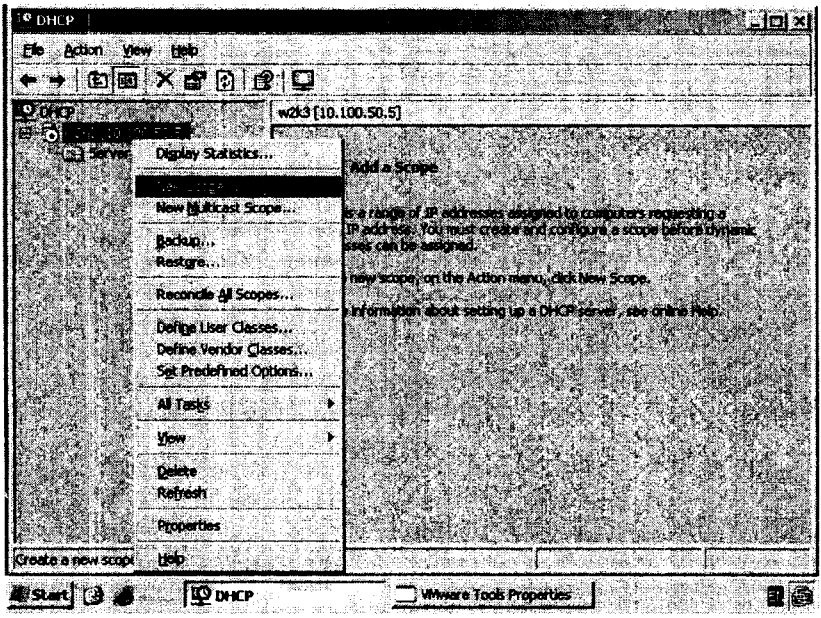
Simvol	**Ünvanlar diapazonu**	**Avadanlığın sayı**	**Diapazonların təyinatı**
B begin	192.168.25.0	0	Şəbəkə avadanlığı üçün tətbiq olunmur
S server	192.168.25.1 - 192.168.25.15	15	Mövcud və təxmin edilən serverlərin ünvanları

P printers	192.168.25.16 - 192.168.25.25	9	Mövcud və təxmin edilən print-serverlərin ünvanları
R routers	192.168.25.26 - 192.168.25.50	25	Şəbəkələrarası əlaqələrdə olan qurğuların ünvanları
F fixed	192.168.25.51 - 192.168.25.99	49	Şəbəkəyə məxsus IP ünvanları dəqiq müəyyən olunmuş kompüterlərin ünvanları
D dynamic	192.168.25.100 - 192.168.25.220	121	Şəbəkəyə məxsus və ünvanları DHCP serveri tərəfindən təyin olunan kompüterlərin ünvanları
X	192.168.25.221 - 192.168.25.244	24	Bronlaşdırılmış ünvanlar diapazonu
E end	192.168.25.255	0	Şəbəkə avadanlığı üçün tətbiq olunmur

1.6 DHCP serverinin sazlanması

Cari fəslin bu bölməsində konkret korporativ şəbəkə üçün MS Windows Server 2003 əməliyyat sistemi əsasında artıq sazlanmış DHCP serveri göstərilmişdir. Müxtəlif şəbəkələrdə əsas

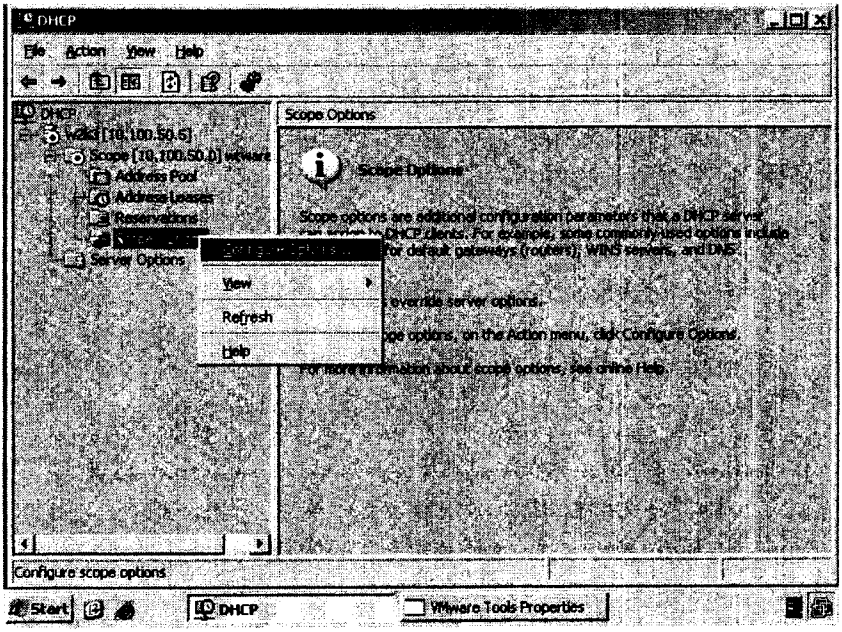
serverlərin adlarında müxtəlif olur. Digər yazılı parametrlər və sazlamalar fərqlənə bilər. Əgər serverin sazlanmasında hər hansı parametri dəyişmək lazımdırsa, bu prosedura yerinə yetirildikdə aparılan dəyişikliklər haqqında yazılı qeydlər edilir ki, sapmalar zamanı serveri ilkin vəziyyətə qaytarmaq mümkün olsun. MS Windows Server 2003 əməliyyat sisteminin DHCP idarəetmə (DHCP Administrating) pəncərəsi şəkil 1.2-də göstərilmişdir.



Şəkil 1.2 DHCP pəncərəsi

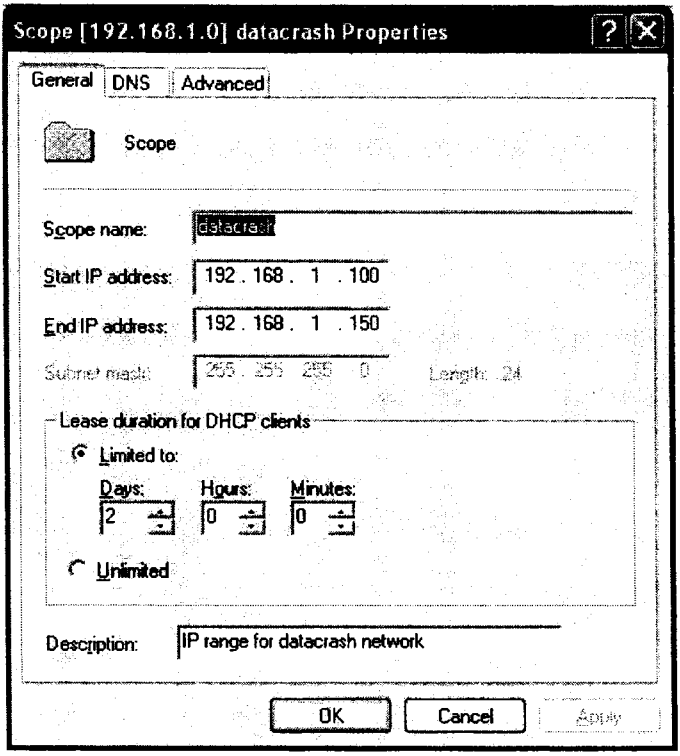
Bu pəncərənin sol hissəsində yerləşən göstərici verilən serverin IP ünvanıdır. Bu pəncərədə obyekti açdıqda oblast və server parametrlərinin göstəriciləri qovluğu ekrana çıxacaq. Pəncərənin lazım olan parametrləri və obyektləri server quraşdıran zaman sazlanmışdır. Buna baxmayaraq seçilmiş siyasətə uyğun olaraq ünvanların bölüşdürülməsini sazlamaq vacibdir. Bunun üçün oblast qovluğunu çevirərək ünvanlar seli tapılır (şəkil 1.3).

Pəncərənin sağ hissəsində kirayə üçün ünvanlar diapazonu əks olunacaqdır. Bu diapazonlardan olan ünvanlar DHCP serverindən korporativ şəbəkənin işçi stansiyalarına veriləcəkdir. Bu diapazonu dəyişmək üçün yenidən oblastı dəyişdirmək və menyuda DHCP pəncərəsində "xassələr" bəndini seçmək lazımdır.



Şəkil 1.3 DHCP pəncərəsi - tam açılmış menyu ilə

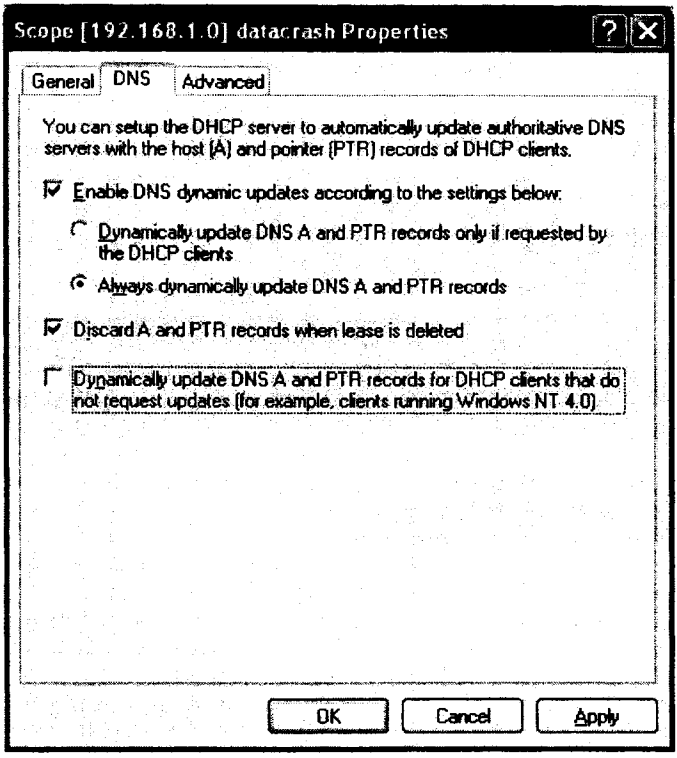
Şəkil 1.4-də verilmiş xassələr pəncərəsində oblastın adını onun başlanğıc və son ünvanlarını, həmçinin ünvanın kirayə müddətini dəyişmək mümkündür. Kirayə müddətini o vaxt təyin edirlər ki, bu müddət ərzində həmin ünvan işçi stansiyaya "təhkim" olunur və o uzun müddət şəbəkəyə daxil olmur. Başlanğıc və son ünvan oblastları yalnız bu seçimdə deyil həm də oblastın özünün xassələrindən asılı olaraq məhdudlaşa bilər.



Şəkil 1.4 DHCP pəncərəsində xassələr bəndi

Misal üçün əgər bir neçə altş əbəkə yaratmaq lazımdırsa, onda onlar hamısı altşəbəkə maskasına malik olmalıdırlar və "255.255.255.0" ünvanından fərqlənməlidirlər ki, başlanğıc və son ünvanlar maskaya uyğun olaraq təyin olunsun. Bu halda bir altşəbəkə üçün ünvanların diapazonunun maksimal imkanlarından istifadə olunur, lakin başlanğıc və son ünvanlar oblastı qoyulmuş şərtlərə əsasən administrator tərəfindən seçilir. Belə şəraitdə şəbəkə ünvanlarının dinamik seçilməsi (bax cədvəl 1.1) "192.168.25.100 – 192.168.25.220" diapazonunu əhatə edir ki, bu da "192.168.25" verilmiş şəbəkənin ünvanına uyğun gəlir. DHCP–serverinin işi, DNS serverin işi ilə çox sıx əlaqəlidir. Buna

görə də DNS pəncərəsinin (şəkil 1.5) xidmətlər bölməsində serverin işində bir neçə parametri dəyişmək olar. Əgər serverin işində hər hansı bir çatışmamazlıq hiss olunarsa, onda yaxşı olar ki, sazlama şəkil 1.5-də olduğu kimi saxlanılsın.



Şəkil 1.5 DHCP pəncərəsində DNS bəndi

MS Windows Server 2003 əməliyyat sistemi əsasında DHCP serveri quraşdırıldıqdan və sazlandıqdan sonra şəbəkənin kompüterinə ünvanlar verilməyə başlanılır. Bu şərtlə ki, hər işçi stansiyada sazlama zamanı TCP/IP protokolu bölməsində: "IP ünvanını avtomatik alınsın" bəndini seçirik. Bunun nəticəsində verilən ünvanları MS Windows Server 2003 əməliyyat sistemində olan "DHCP" pəncərəsində görmək mümkündür. Bunun üçün

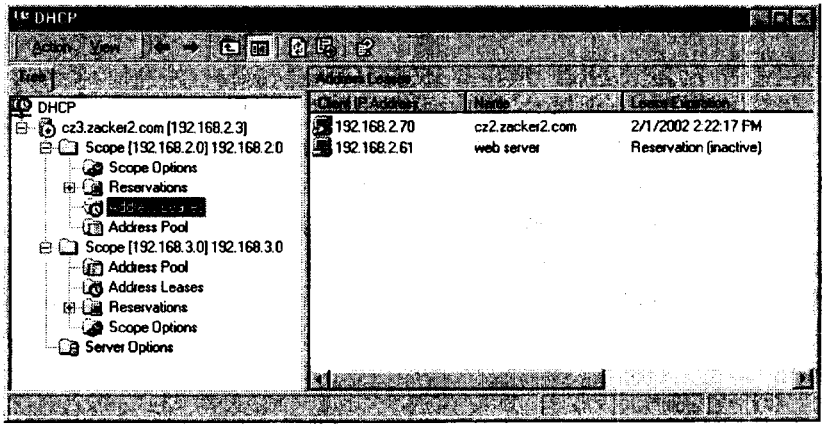
kirayəli ünvanlar oblastını qeyd edərək, açılmış oblastlar ağacına və pəncərənin sağ tərəfinə baxmaq lazımdır. Orada, kimə hansı ünvan, hansı vaxta qədər verilməsi barədə tam dolğun informasiya ilə tanış olmaq olar. Əgər MS Windows Server 2003 əməliyyat sistemi əsasında sazlanmış DHCP-serveri korporativ şəbəkədə işləyirsə və yalnız verilən ünvanların diapazonunu dəyişmək qərarı verilibsə, onda sazlama aparmadan öncə kirayəli ünvanlara baxmaq lazımdır. Əgər onlardan bir neçəsi seçilmiş diapazondan kənara çıxarsa, onda iki yolla getmək mümkündür:

- Server tərəfindən verilən ünvanların diapazonlarını artıq verilənlər tərəfə yerləşdirmək lazımdır. Bu halda cədvəl 1.1-də düzəlişlər edilməsi tələb olunur.
- İşçi stansiyasının ünvanını kirayələnmiş ünvanların siyahısından silməkdən ötrü, onu "D" diapazonunun əhatəsindən kənara çıxaraq işinin qurtarmasını gözləmək lazımdır. Ünvanların başlanğıc və son diapazonları quraşdırıldıqdan sonra server yenidən işçi stansiyalara onların ünvanlarını şəbəkəyə çıxan kimi, artıq müəyyən olunmuş diapazonlar əsasında verəcəkdir.

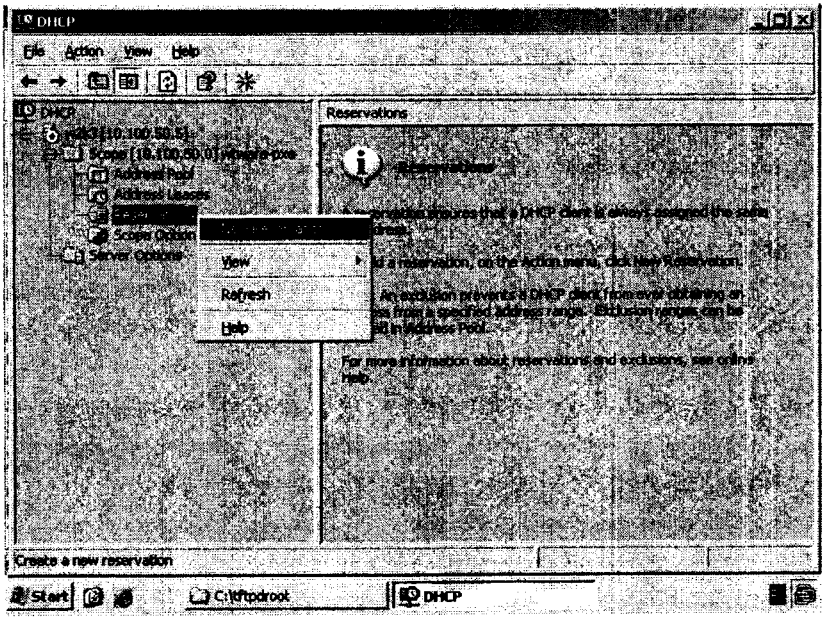
Şəkil 1.6-da pəncərənin sağ hissəsində kirayə vaxtının qurtarması xanasında bir neçə işçi stansiyaların aktiv və ya passiv kirayə vaxtı üçün "ehtiyatlar" bəndi görünür. Bu kirayə üçün ehtiyatlar vaxtı lazım gəldikdə isə MS Windows Server 2003 əməliyyat sistemi əsasında sazlanmış DHCP-serverinin xidmətindən istifadə edərək işçi stansiyası öz ünvanını dəyişir və hətta şəbəkədən uzun müddət ayrıla bilər. Başqa sözlə ünvanın kirayə müddətinə korporativ şəbəkənin işçi stansiyaları üçün məhdudiyyət qoyulmur.

Ünvanların ehtiyatlaşdırılması üçün Şəkil 1.7-də göstərilən pəncərənin sol hissəsində ehtiyatlaşdırma bəndini açaraq və pəncərənin sağ hissəsində ünvanlar siyahısına baxmaq olar. Yeni ehtiyatlaşdırma yaratmaq üçün menyuda "DHCP" pəncərəsində yeni ehtiyatlaşdırma yaratmaq bəndi seçilir. Bu proseduradan

öncə həmin işçi stansiyanın "MAC–ünvanına" (Media Access Control) baxılır və burada ehtiyatlaşdırma yaradılır.



Şəkil 1.6 DHCP - kirayələnmiş ünvanlar



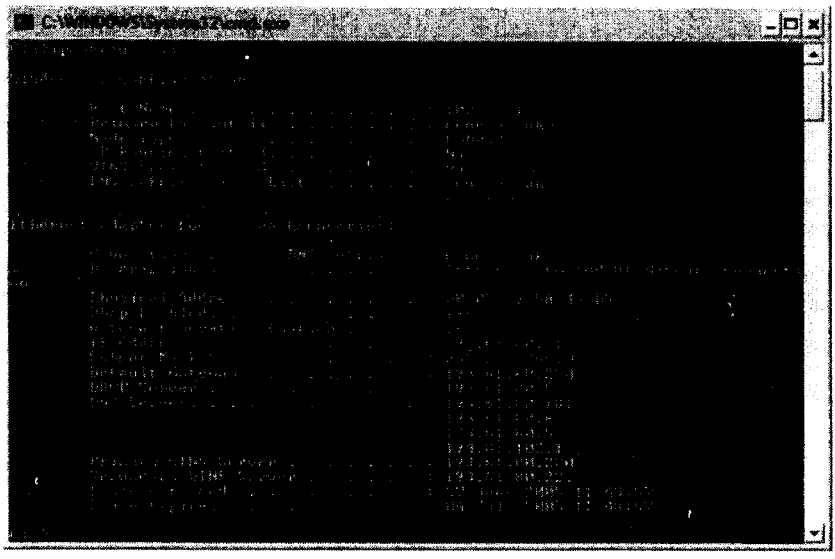
Şəkil 1.7 DHCP - kirayələnmiş ünvanlar

MAC–ünvanı - 48 baytlı ünvan, şəbəkə kartını hazırlayanların əlavəsidir. Bu ünvan IP ünvanını soraqlayan maşının identifikasiyası üçün istifadə edilə bilər. Ehtiyatlaşdırma yaradılan zaman onu arakəsməsiz və defissiz göstərmək tələb olunur. Komanda sətri pəncərəsində "ipconfig /all" komandasını yerinə yetirərək MAC-ünvanını tanımaq olar. Ekrana (şəkil 1.8) IP protokolunun nizamlanması haqqında məlumat gələcəkdir və fiziki ünvan sətrində bu kompüterin MAC-ünvanı göstərilir.

Şəbəkə ən etibarlı proqram və aparat təminatı ilə təchiz olunsa belə, bir neçə şərtlər yerinə yetirilmədən, onların effektiv tətbiqi qeyri real olar. Belə ki, şəbəkənin uzaqdan idarə olunması üçün ya İnternetə çıxış olmalıdır və ya şəbəkədə olan maşınlardan birində uzaqdan idarəetməni təmin edən server qoşulmalıdır. Ən yaxşı variant – bu daimi İnternet əlaqəsidir, odur ki, biz bu varianta baxacağıq.

Belə qoşulmanın konkret fəaliyyəti administratorun imkanlarından və xidmət sayından, regionda İnternet xidmətindən istifadənin hansı səviyyədə olmasından asılı olacaq. Kitabda əsas variant kimi "ADSL"–modemi vasitəsi ilə qoşulmağa baxılır çünki, o ən çox yayılmış üsullardan biridir və onun köməkliyi ilə hətta ev şəraitində belə qlobal şəbəkələrə qoşulmaq mümkündür. Əgər bu qoşulma təşkil olunmayıbsa, müvəqqəti olaraq bu işi adi modemlə də həyata keçirmək olar. Lakin bu halda verilənlərin ötürülmə sürəti çox aşağı olur ki, bunun nəticəsində də olduqca az sayda istifadəçilərə İnternet xidməti göstərmək mümkün olur. Buna baxmayaraq modem birləşməsi şəbəkəyə kənardan qoşulmaq üçün instrumental vasitə kimi istifadə oluna bilər.

Korporativ şəbəkədə IP ünvanlarının paylanma siyasətinin necə təşkil olunmasında asılı olmayaraq, kompüter administratorla daimi IP ünvanına malik olmalıdır. Bu halda "ADSL", İnternet şəbəkəsinə tam hüquqlu girişə şərait yaradır və həmçinin bir sıra digər problemləri həll edir.



Şəkil 1.8 Komanda sətri – "ipconfig /all" əmrinin nəticəsi

Şəbəkə istifadəçilərinin böyük əksəriyyəti, işə başlayanda kompüterin qoşulması zamanı avtorizasiya proseduralarından və şəbəkədə qeydiyyatdan keçir. Bu zaman istifadəçilər yalnız öz şəbəkələrinin daxilində deyil, həm də avtonom rejimində işləməli olacaqlar. Bu halda istifadəçilər şəbəkədə qeydiyyatdan keçə bilmir və administrator hüququnda sistemə daxil ola bilmirlər. Kompüteri işə salandan sonra iş zamanı ayrı-ayrı vəziyyətlərdə, avtorizasiyanın müxtəlif proseduralarını tətbiq etmək üçün həmişə lokal şəbəkə administratorunun kompüterində avtorizasiyadan keçmək lazımdır. Bundan sonra əməliyyat sistemi MS Windows XP şəbəkə əlavələrinə buraxmaq imkanını təmin edir və şəbəkədə avtorizasiyadan keçdikdən sonra resurslara giriş əldə etməyə şərait yaradır. Bu qaydalara riayət olunduqda, müəyyən səbəblər üzündən kompüter işləyərkən istifadəçi ondan aralanarsa həmin an onun kritik şəbəkə resurslarına icazəsiz girişlərinin qarşısını almaq üçün əlavə mühafizə imkanları mövcuddur.

Yalnız bəzi hallarda, məsələn MS Windows vasitələri ilə işçi stansiyaları və şəbəkəni idarə edən zaman, domen administratorunda qeydiyyatdan keçməsi tələb oluna bilər. MS Windows XP əməliyyat sistemi elə şərait yaradır ki, kiminsə adından sistemə daxil olub, parolu əvvəlcədən məlum olan şəbəkənin hər hansı bir istifadəçisinin proqramlarına girmək mümkün olsun. Hal hazırda MS Windows seansında necə qeydiyyatdan keçməsindən asılı olmayaraq, server və ya domen administratoru adından fayl menecerində pəncərə açmaq mümkündür və bunun vasitəsi ilə istifadəçilərin apara bildikləri bütün əməliyyatları orada izləməmək olar.

1.7 Lisenziya siyasətinə əməl olunması

Əfsuslar olsun ki, hal-hazırda bir çox təşkilatların başçıları ilə proqram məhsulları hazırlayan mütəxəssislər arasında, proqram təminatını qiymətləndirilməsində, proqrama lazımi vəsait qoyuluşunda fikir ayrılığı yaranır. Praktikadan məlum olduğu kimi, təşkilatlar köməkçi proqramlar almaqdansa yeni avadanlıqların alınmasına üstünlük verir. Ayrı-ayrı hallarda yeni "OEM" kompüterlərə quraşdırılmış proqram versiyalarının köməyi ilə vəziyyəti bir qədər sadələşdirmək olar. Digər hallarda isə alternativ bir variant kimi çıxış yolu axtarmaq lazım gəlir, bunun üçün şərti pulsuz və ya tam pulsuz proqramlardan istifadə olunur. Ola bilsin ki onlar kommersiya baxımından tam funksional olmasın. Lakin onları tətbiq etdikdə, onu çox dəqiq testdən keçirərək onun incə nöqtələrini təyin etmək olar və çatışmayan cəhətlərini zərərləşdirərək, ciddi nəticələrə nail olmaq olar. Ayrı-ayrı hallarda administratorunda bu prosesə qoşulması lazım gəlir.

Bunu da bilmək lazımdır ki, pulsuz istifadə üçün məhdudiyyət vaxtı 15 gündən 45 günə qədərdir. Razılaşsaq ki, bu müddət ərzində olduqca ciddi işləri həll etmək mümkündür və nəticədə onları qiymətləndirərək əldə etmək olar. Ayrı-ayrı

kateqoriyalı istifadəçilər üçün bir neçə proqram təminatları pulsuzdur. Məsələn fayl meneceri "FAR", MDB ərazisində yaşayan əhali üçün pulsuzdur. Lakin lisenziyalı proqram təminatları administratorları çoxlu problemlərdən azad edərək, proqram təminatını təşkilatın funksional-texniki tələblərinə uyğunlaşdırmasına yardımçı olur. Müasir korporativ şəbəkələrin idarə olunması praktikasına əsaslanaraq demək olar ki, proqram istehsalçılarının böyük bir hissəsi, özlərinin leqal istifadəçilərinə çox böyük diqqət yetirirlər. Əgər sistem proqramlar lazımlı, lakin az sayda məsələlərin həllinə tətbiq olunmaqdan ötrü hazırlanıbsa, yalnız leqal istifadəçi kimi proqramın funksionallığını təkmilləşdirilməsində administratorlar öz konstruktiv təkliflərini və düzəlişlərini verə bilər ki, proqram təminatını istehsalçıları hökmən bu təklifləri nəzərə alsınlar. Bununla da istifadəçilər tərəfindən verilən təkliflər əsasında yaranmış və lazım olan yeni təkmilləşdirilmiş proqramlar istifadə üçün təqdim olunur. Ona görə də yeni proqramlarla işləməyə başlayan zaman lisenziya razılaşmalarının müddəaları ilə diqqətlə tanış olmaq lazımdır.

1.8 Real şəbəkənin praktik tərəfi

Şəbəkədə idarə etmə məsələlərinə baxmazdan öncə, şəbəkənin özü ilə tanış olaq. Fəslin başlanğıcında server otağının fraqmentləri göstərilmişdir. Bunu bir də təkrar etməyə heç bir ehtiyac yoxdur. Çünki kompüter–bütün hallarda kompüterdir, onun hansı modeldə olması və ya hansı stolda qoyulması az maraq doğurur. Lakin şəbəkənin strukturu isə olduqca diqqət mərkəzində olmalıdır. Şəbəkə dərhal, yəni tez bir zaman kəsiyində yaranmır, şəbəkəni genişləndirmək məqsədi ilə bilmədən hər hansı administrator qaydalara zidd olaraq öz əlavələrini edə bilər. Odur ki, şəbəkədə iş yerlərinin təşkili zamanı bütün normalara ciddi əməl olunmaması ən vacib məsələlərdən biridir.

Artan nömrəli sayla şəbəkə fraqmentlərinin şəkillərini düzərək (şəkil 1.9-1.11) şəbəkə haqqında məlumatlara yiyələnmək

olar. Şəkillərdə şəbəkənin əsas komponentləri təsvir olunmuşdur. İşçi stansiyaların bir çox hissələri və konstruktiv həlli göstərilməmişdir. Buna baxmayaraq şəkillərdə işləyən şəbəkənin konkret qurğularına baxmaq üçün bəs qədər informasiya vardır. Diqqət yetirmək lazımdır ki, şəbəkənin bütün sahələri fasiləsiz cərəyan mənbəyi ilə təchiz olunsun, elektrik təchizatında olan qısa fasilələr zamanı və gərginliyin azalması zamanı etibarlı funksional iş rejimi təmin olunsun. Serverin bütün avadanlıqları (şəkil 1.9) fasiləsiz cərəyan mənbəyinə qoşulur. Digər sahədə isə fasiləsiz cərəyan mənbəyinə daha vacib funksiyalar yerinə yetirən kommutatorlar və işçi stansiyalar qoşulur. İdeal şərait yaratmaq məqsədi ilə yaxşı olardı ki, bütün qurğular fasiləsiz cərəyan mənbəyinə qoşulsun, lakin xərcləri və itkiləri nəzərə alaraq fasiləsiz cərəyan mənbəyə qoşulma optimal variantda aparılır. Fasiləsiz cərəyan mənbəyinin quraşdırılmasının vacibliyinə baxılan zaman, dəyən ziyanı nəzərə almaq lazımdır çünki, bu zaman qəflətən bu və ya digər kompüterlər dayana bilər. Şəkildə işçi stansiyanın konkret təyinatı göstərilməyib, ona görə də şəbəkədə fasiləsiz cərəyan mənbəyinin hansı sahəsində qurulmasını administrator təyin edir. Şəkildə göstərilənlər haqqında aşağıdakıları şərh etmək olar. Şəkil 1.9-un yuxarı hissəsində server otağına aid olanlar göstərilib. Şəkildə administratorun iş yeri göstərilməyib çünki, əgər o portativ kompüter olarsa, onun qoşulması üçün xüsusi şərait tələb olunmur. Bu kompüterin İnternetə çıxışı olduğu üçün onu işçi stansiya kimi qəbul etmək olar. Şəbəkənin baş serveri – MS Windows 2000 Server əməliyyat sistemi ilə idarə olunaraq (şəkil 1.9) şəbəkəyə yeganə şəbəkə adapteri vasitəsi ilə qoşulur.

MS Windows Server 2003 əməliyyat sistemi ilə işləyən ikinci server iki şəbəkə adapterinə malikdir, onlardan biri şəbəkəyə birləşdirilir, digəri – ADSL modeminə (Asymmentric Digital Subscriber Line, asimmetrik rəqəmli abonent xətti) qoşularaq şəbəkə istifadəçilərinin İnternetə qoşulmasına şərait

yaradır. Serverin IP ünvanları "S" diapazonundan seçilir (bax cədvəl 1.1). Hər iki server bir monitor və klaviaturadan istifadə edir. Bunlar serverə kommutator vasitəsi ilə birləşirlər. Bu həm monitorun həm də serverin alınmasına qənaət etməyə imkan yaradır. Serverə iki telefon xətti gəlir. Biri adi, digəri isə ayrılmış optik xətt ilə başqa lokal şəbəkə ilə rabitə yaradır. Bu rabitə adi analoq modem vasitəsi ilə həyata keçirilir. Marşrutizator öz növbəsində kommutator (şəkildə Kommutator 1 kimi işarələnmişdir) vasitəsi ilə şəbəkəyə qoşulur. Həmçinin serverlər də kommutatora birləşdirilir. Nöqtələr sayını artırmaq üçün kabel xəttinə ikinci kommutator tətbiq olunur. Onun qoşulmasının vacibliyi server kabellərindən və əlavə kanalların sayından asılıdır. Ola bilsin ki, şəbəkədə bir kommutator bəs etsin, real şəbəkələr əsasında çəkilən bu şəkildə üç kommutator durur. Kommutator kabelləri binanın mərtəbələrinə və digər tərəflərə serverdən uzaq məsafələrə paylanır. Şəkil 1.10-da xətlərdən biri göstərilib - ayrılmış xətt. Bu kabelin uzunluğu 100 metrdən çoxdur, şəkil 1.11-də görürük ki, o adi hab (hub) qurğusuna keçərək gücləndirici rolunu oynayır, sonra kabel yenə 100 metr uzadılaraq və yeni hab qurğusu quraşdırılır. Buna da bir neçə kompüter qoşulur. İkinci habın qabağında kabel düyünü durur. Bu kabelin ehtiyatı olub, keyfiyyətli rabitə əldə etmək üçün, lazım gəldikdə onun uzunluğunu artırıb azaltmaq məqsədi güdür. Əgər kompüter birinci dəfə işə salınarkən şəbəkəyə girişdə hər hansı problem müşahidə olunarsa, onda kabeli tədricən qısaldaraq (təxminən bir dəfə 50 sm.), hər dəfə rabitəni yoxlamaq lazımdır. Kabellərdən ən çox 2.5 metrə yaxın kəsərək və kompüterin normal funksiyalılığını əldə etmək olar. Vacib məsələlərdən biri odur ki, bu uzun kabel keçdiyi yerlərdə yüksək gərginlikli xətlər olmasın, əks təqdirdə ondan yaranan maqnit sahəsi bu xəttin işləməsinə imkan verməz. Bir çox binalarda şəbəkə kabelləri girişi olan xüsusi təyinatlı qutulara qoyulur. O məqsədlə ki qoşulma zamanı digər mərtəbələrdə qoşulma nöqtələri çatışmadıqda, əlavə

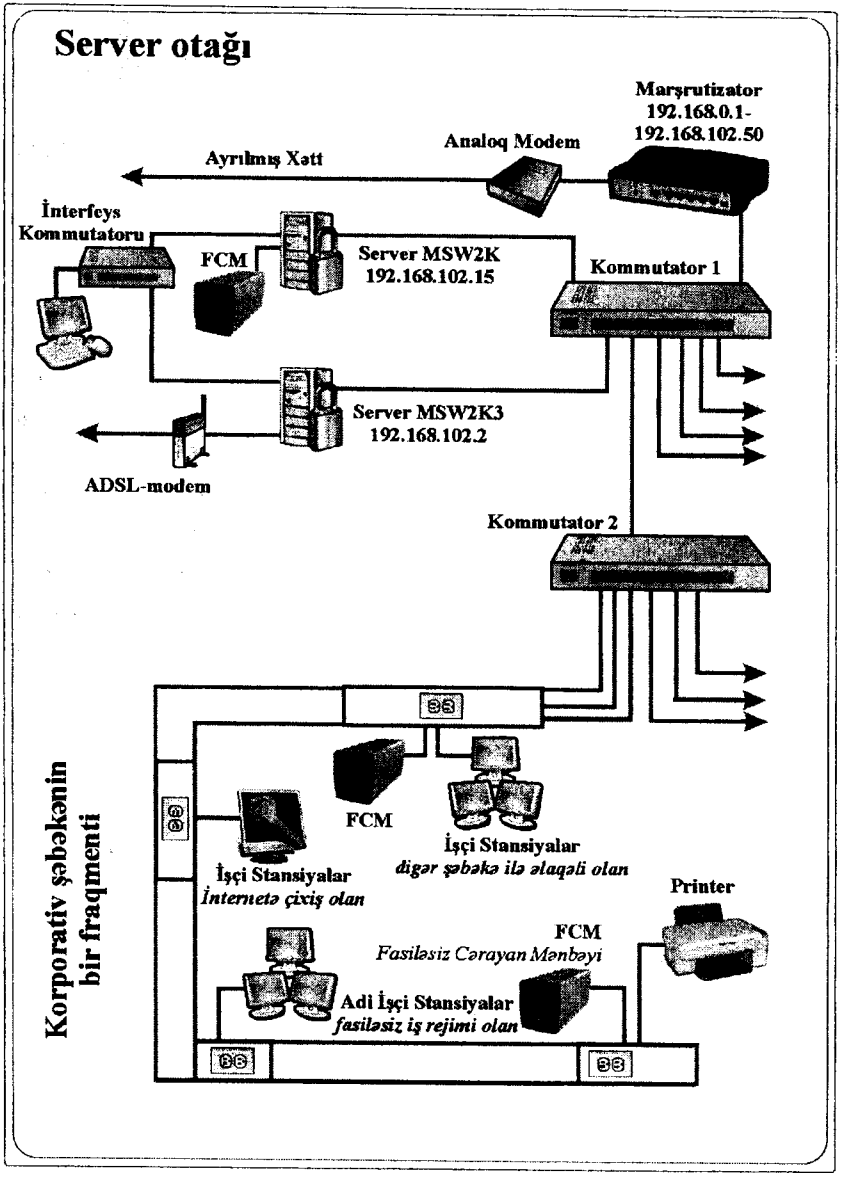
olaraq kommutatorlar qoyulması mümkün olsun. (şəkil 1.10-da Kommutator 3 kimi işarələnmişdir) Bu da mərtəbədə bir neçə xətti birləşdirməyə imkan yaradır. Əgər print-serverə şəbəkə printerlərini qoşmaq tələb olunursa, onda onları adi kompüter kimi qoşurlar (şəkillərdə "Printer" kimi işarələnib). Qeyd etmək lazımdır ki, işçi stansiyanın təyinatından asılı olmayaraq, onun lokal şəbəkəyə qoşulması üsullarına heç cür təsir etmir. Ona görə də biz gələcəkdə iş prinsipinə baxdıqda onun qurğularına, kabel qoyuluşu üsullarına və işçi stansiyalıların qoşulmasına qayıtmayacağıq. Təmas nöqtələrinin keyfiyyətsiz birləşməsi üzündən problemlərin olmaması üçün, bütün işlərin keyfiyyətli yerinə yetirilməsi və birləşmələrin etibarlı olması vacib şərtlərdən biridir. Kabelin keçdiyi yerin düzgün seçilməsi çox böyük əhəmiyyət kəsb edir. Texniki və nəzəri cəhətdən şəbəkəyə ayrılmış xəttin necə qoyulmasının böyük əhəmiyyəti vardır. Qoşulma düzgün aparılarsa, şəbəkənin genişləndirilməsi zamanı çəkiləcək xərcləri kəskin şəkildə azaltmış olar.

Lokal şəbəkələri idarə etmək üçün qeyd etmək lazımdır ki, şəbəkə serveri ilə işçi stansiyaların təyinatlarına görə bir birindən ayırmaq vacibdir. İşçi stansiyaların statusuna görə şəbəkədə imkanları bir qədər məhduddur. Serverin spesifik tapşırığı onun fasiləsiz işləməsini tələb edir. Bu o deməkdir ki, serverin söndürülməsi və yenidən işə salınmasını yol verilməzdir. Buna baxmayaraq şəbəkə administratorunun işi zamanı, şəbəkədə kiçik dayanmalar üzündən onun işinə ziyan gətirən bu cüzi vaxt intervallarını, yenidən işə salınma və ya serverin söndürülməsinə sərf olunan vaxtları təyin etmək lazımdır. Əgər şəbəkə istifadəçiləri bu vaxt şəbəkədə işləyərlərsə, onlar bu riskli momentdə yaddaşda olan verilənləri itirə bilərlər və ya şəbəkə servisinin imkanlarında tam istifadə edə bilməzlər. Bu dövrlər maksimum şəkildə azaldılmalıdır. Hər hansı bir təşkilata məxsus şəbəkənin profilaktik texniki proseduralarını istirahət günləri etmək məqsədə uyğundur. Buna baxmayaraq bu işlərin yerinə

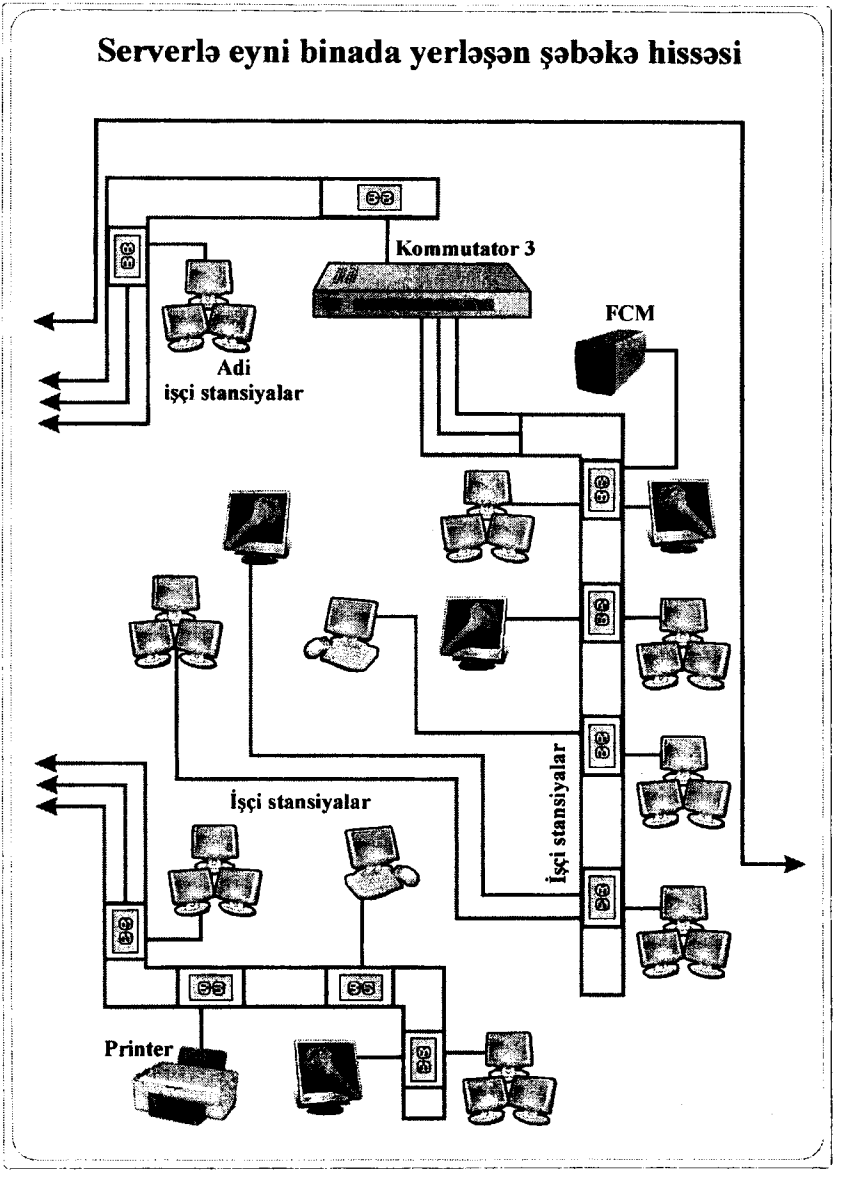
yetirilməsinə ayrılan vaxt ərzində şəbəkədə işəyən istifadəçiləri müəyyən edib, onlara yarana biləcək fasilə haqqında xəbərdarlıq etmək lazımdır.

Əgər administratorun sərəncamında bir deyil, bir neçə server vardırsa, onda onların yeni əvəzedici serverlərin funksiyalarını qaldırıb şəbəkənin fasiləsiz iş rejimini yüksəltmək olar. Məsələn ikinci serverdə DNS xidmətini quraşdırmaq çox asandır. Bunun üçün əsas serverdən baxış zonası köçürülür və sinxronlaşdırma nizamlanır. Bununla belə istifadəçilərin işçi stansiyalarının lazım gəldikdə bu serverə müraciət etmə imkanı olmalıdır, yəni o bunlara bir alternativ kimi olmalıdır. Hər hansı kompüterlə bir az iş səriştəsi olan istifadəçi bilməlidir ki, verilənlərin ehtiyat nüsxəsini mütəmadi olaraq digər mənbədə saxlamaq lazımdır. Hər şeydən əvvəl bu proseduranı işçi stansiyalar üçün düzgün yerinə yetirmək lazımdır, məsələn məlumatların müxtəlif tip daşıyıcılarda, disklərdə arxivləşdirmək vacibdir. Bununla yanaşı serverin özündə və şəbəkə diskində də arxiv yaradılır. Serverin ən yüksək etibarlılığına baxmayaraq, sapmaların ehtimalı daim vardır, hətta real praktikada sapmalar nəticəsində verilənlərin itirilməsi ilə qarşılaşmaq mümkündür. Belə hallara həmişə hazır olmaq lazımdır.

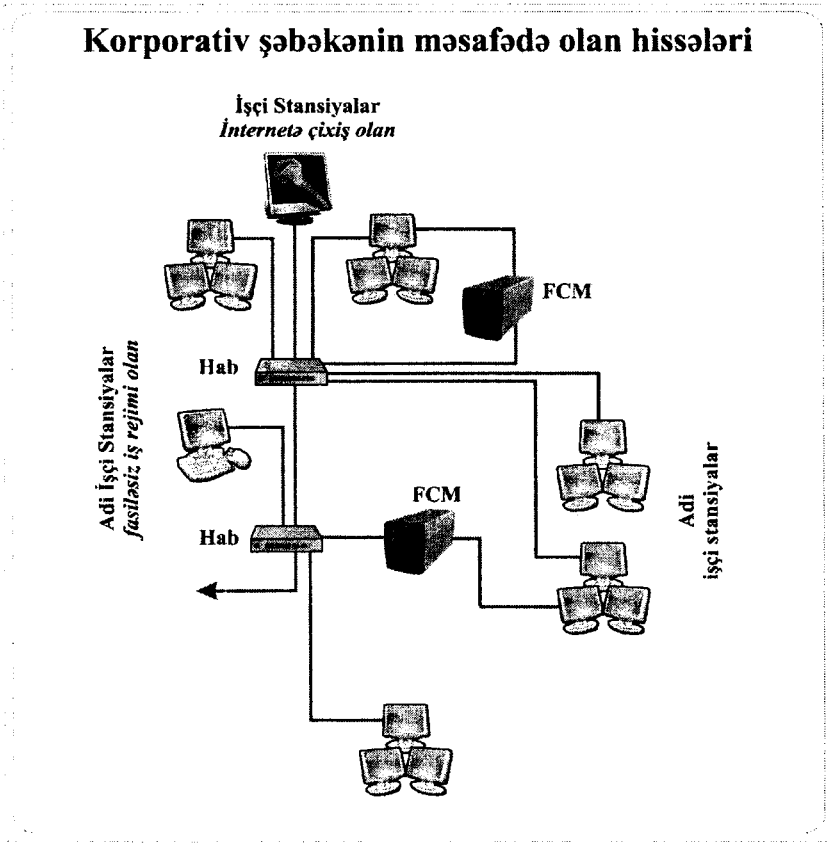
Qəza. Korporativ şəbəkənin idarə olunması zamanı yarana biləcək problemlər silsiləsindən birini nəzərdən keçirək. Şəbəkənin adi iş rejimində heç bir səbəb olmadan MS Windows 2003 Server əməliyyat sisteminin yüklənməsində problemlər yarana bilər. İlk baxışdan serverin yükləmə prosesində əməliyyat sistemi Active Directory kataloqunun xidmətdən imtina etdiyini bəyan edir.



Şəkil 1.9 Şəbəkə fraqmenti 1



Şəkil 1.10 Şəbəkə fraqmenti 2



Şəkil 1.11 Şəbəkə fraqmenti 3

Əməliyyat sistem tərəfindən təklif olunan kataloqun yenidən bərpa olunması xidməti heç bir nəticə vermir. Arxiv sistemi və arxiv obrazlı disk yaratmaq mümkün olmur. Bu zaman şəbəkənin administratoru tərəfindən aparılan monitorinq nəticəsində məlum olur ki, şəbəkənin DNS-serveri və DHCP-serveri işləmir, daha doğrusu düzgün işləmirlər və şəbəkə istifadəçiləri məhz bu səbəbdən sistemə daxil ola bilmirlər və Active Directory kataloqunu bərpa etmək mümkün olmur. Şəbəkənin düzgün işləməməsi səbəbini müəyyənləşdirdikdən

sonra sistem administratoru imkan daxilində DNS-serveri və DHCP-serverinin işini nizamlamağa çalışmalıdır. Əgər bu bir nəticə vermirsə, onda əməliyyat sistemini ya bərpa etmək, ya da yenidən quraşdırmaq lazım gələcəkdir. Belə problemlərin meydana gəlməsinin əsas səbəblərindən biridə sistem administratorunun vaxtaşırı olaraq funksional-texniki tədbirlərin yerinə yetirməməsidir.

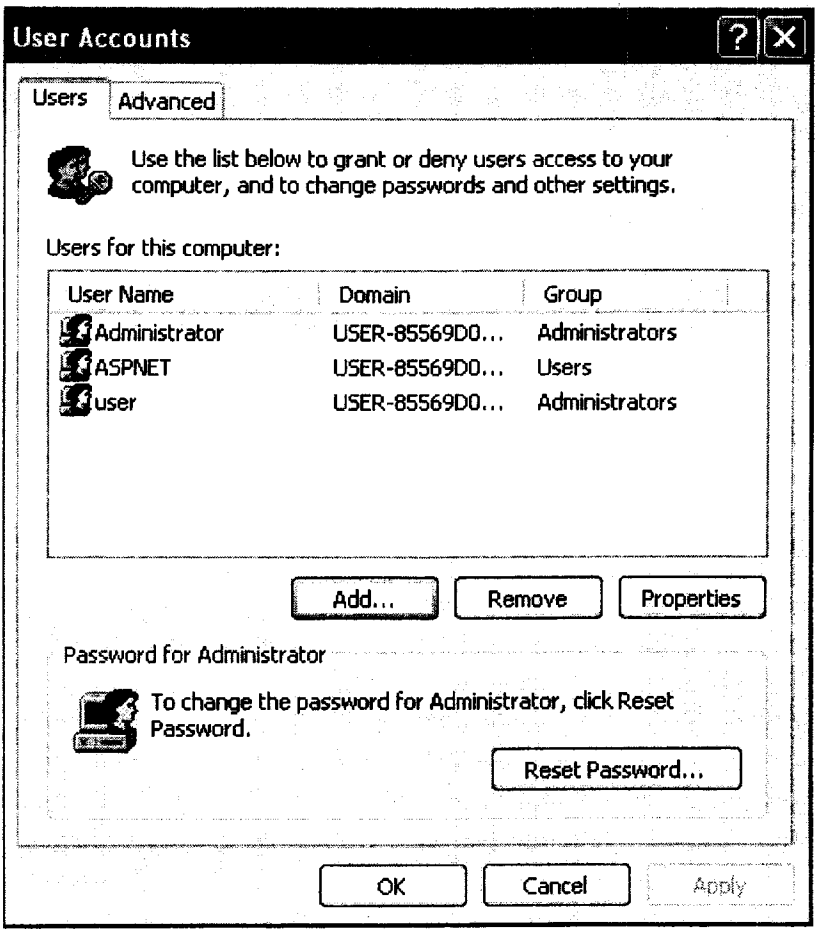
Təkhüquqluluq. Server şəbəkənin idarə olunmasını əsas qaydalarını təyin edir. Kiçik şəbəkələri bir administrator idarə etməlidir. Əlbəttə, köməkçi olmalıdır və ona şəbəkənin idarə olunmasında, ayrı-ayrı məsələlərin həllində hüquq verilir, buna baxmayaraq şəbəkənin işinə bütünlüklə administrator cavabdehdir. MS Windows Server 2003 əməliyyat sistemində istifadəçilər heyətində, məsələn bir neçə qrup istifadəçilər təyin olunmuş hüquqlar əsasında işləyə bilərlər. Yalnız burada administratorun işinə heç bir məhdudiyyət qoyulmur. Administratorun ixtiyarı var ki, şəbəkənin idarə etmək üçün istifadəçilərin sayını bir neçə dəfə artırsın, lakin bunu etmək məsləhət görülmür. Çünki kollektiv idarəetmənin nəticəsi çox ağır ola bilər. Hətta administratorlar yüksək klassifikasiyaya malik olsalar belə iş zamanı onların fikirləri üst-üstə düşməyə bilər. Səhvdən heç kim sığortalanmayıb. İş zamanı buraxılan bu səhvlər nəticəsində çox böyük xoşagəlməz hallar yarana bilər ki, bu da şəbəkənin fasiləsiz iş rejiminin pozulmasına gətirib çıxarar. Əgər şəbəkə böyüyürsə, domendə bir necə altşəbəkələr yaranırsa, onda hər altşəbəkənin özünün administratoru olmalıdır. Domen administratoru öz işini ayrı-ayrı xidmət və sistem administratorları ilə razılaşdırmalıdır. Bu gün əgər bir domen və çox böyük olmayan şəbəkə varsa, onda oranın yeganə administratoru olması kifayətdir. Adətən kompüterlərə və şəbəkələrə xidmət işi dövrü xarakter daşıyır. Server və şəbəkə kompüterlərinə texniki qulluq, vacib verilənlərin arxivləşdirilməsi, yaddaşa salınması tələb olunan, verilənlər bazasına qulluq (əgər tətbiq olunursa),

istifadəçilərin uçot qeydlərinin azaldılması və ya çoxaldılması, kompüter şəbəkələri və şəbəkə üzrə aparılan digər xidmət işləri yaxşı olar ki, protokollaşdırılsın. Qəflətən yaranan problemləri operativ həll etməkdən ötrü problemin kökünü tapmaq üçün şəbəkədə baş verən bütün dəyişikliklər haqqında aparılan qeydlər işin həllini tezləşdirər. Məsələn müştərinin kompüterində şəbəkə kartını dəyişdirdikdə bəzən MS Access verilənlər bazasının işində pozuntular yaranır. Əgər təşkilatda xronoloji olaraq şəbəkədə olan dəyişikliklər qeyd olunursa, onda aparılmış qeydləri təhlil etməklə problemi müəyyən etmək olar. İstifadəçilər bütün dəyişikləri öz kompüterlərində qeyd etmək üçün (əgər onlara icazə verilmişsə) hökmən administratorla razılaşdırmalıdırlar. Təhlükəsizlik baxımından bu qeydləri xüsusi ayrılmış jurnalda aparmaq lazımdır. Əgər hər hansı bir kompüterin elektron poçtundan bu xüsusi qeydləri tam əminliklə oxumaq mümkün olacaqsa, onda jurnaldan istifadə etməmək olar. Amma hər dəfə qeydlərdə dəyişikliklər apardıqdan sonra gündəliyin surətini ən azı iki daşına bilən qurğulara və ya disklərə yazılmalıdır. Gündəlik o formada olmalıdır ki, lazım olanda ya onun bir hissəsini və ya bütövlükdə hamısını çap etmək mümkün olsun.

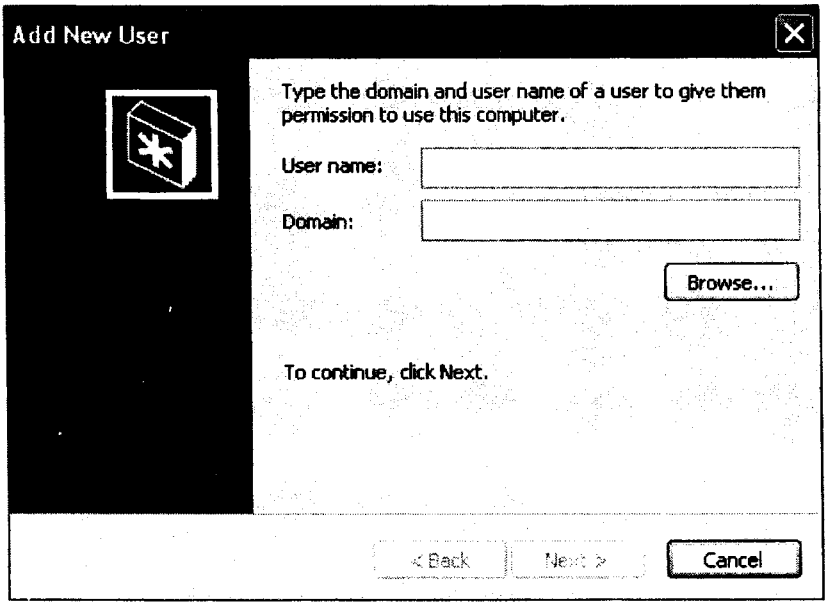
Şəbəkədə olan hər bir kompüterin özünün qeydiyyat yazılarında göstərildiyi kimi onun hər bir istifadəçisi administrator hüququna malik ola bilər. Yaxşı olardı ki, şəbəkə administratoru hər bir işçi stansiyanı nəzarətdə saxlanılsın. Bunun üçün çoxda çətin olmayan bir işi görmək kifayətdir, yəni istifadəçilərin sayını artırmaq lazımdır.

1. Lokal administrator kimi işçi stansiyaların əməliyyat sisteminə daxil olun.
2. İstifadəçilərin uçot qeydlərini açın (şəkil 1.12).
3. Əlavə etmək (Add) düyməsini basın.
4. Görünən pəncərədə (şəkil 1.13) domen administratorunun uçot qeydlərinin adını və domeninin adını yazın.

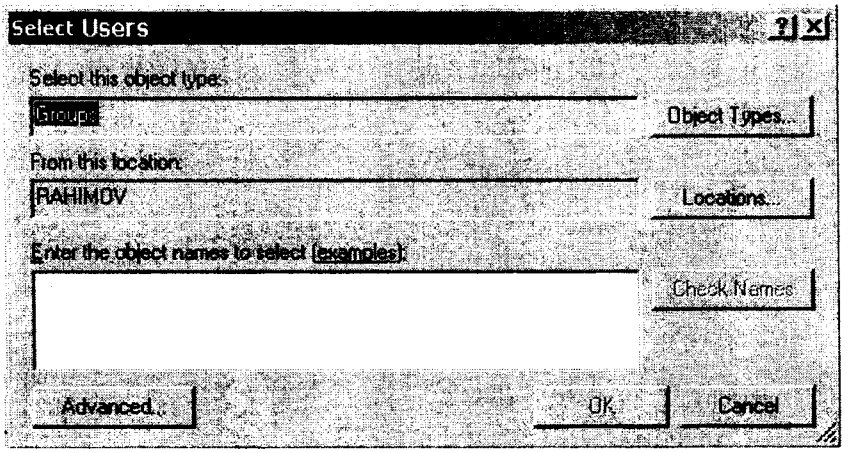
5. Əgər administrator bu adı yadına sala bilmirsə (və ya kompüterə digər qeydiyyat yazıları ilə girişə icazə tələb olunarsa) "Aramaq" (Browse...) düyməsini basın.



Şəkil 1.12 İstifadəçilərin qeydiyyat yazıları

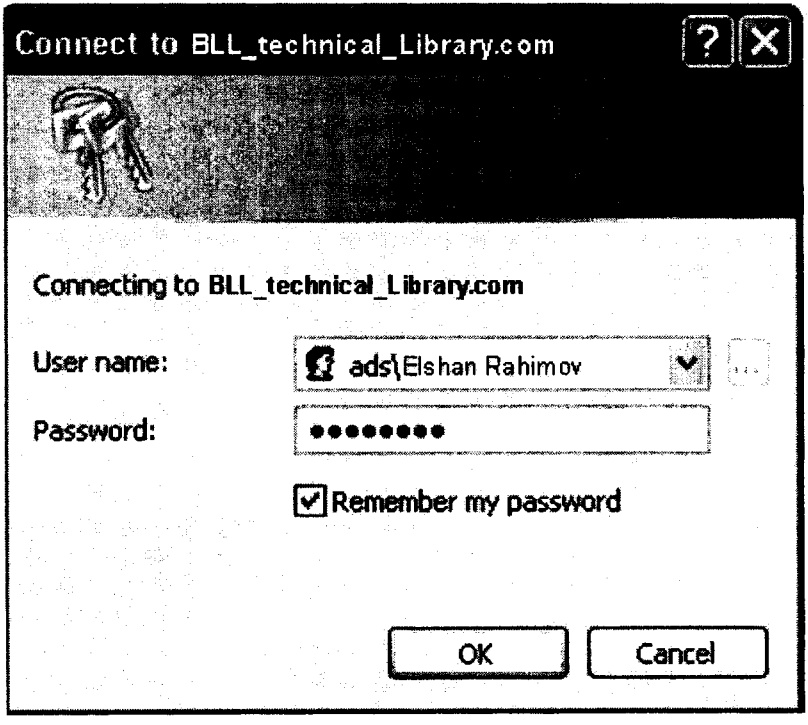


Şəkil 1.13 Yeni istifadəçinin əlavə olunması



Şəkil 1.14 İstifadəçinin seçilməsi

6. Açılmış pəncərədə (şəkil 1.14) "Əlavə" (Advanced) düyməsini basın.
7. Şəkil 1.15-də domen administratorunun adı və parolunu daxil etmək üçün dəvət pəncərəsi əks olunmuşdur. Bu halda istifadəçinin adı: **<domenin adı>/<uçot qeydlərinin adı>** şəklində olur.



Şəkil 1.15 Şəbəkə parolunun daxil olunması

8. Açılmış pəncərədə istifadəçinin seçilməsində "Yerləşdirmə" düyməsini basaraq, ağacda olan obyektlərdən axtarılan istifadəçiləri tapıb və ya "Ad" sahəsində qeydiyyat yazıların ilk hərflərini qeyd edin və "Axtarış" (Find Now) düyməsini basın.

9. "OK" düyməsini iki dəfə, sonra isə "Növbəti" (Next) düyməsini basın.
10. "Yeni istifadəçilərin əlavə olunması" pəncərəsində verilmiş kompüter üçün onun hüququnu seçin.
11. "OK" düyməsini basın və bütün pəncərələri bağlayın. Domen administratorları kompüter administratorlarının sayına əlavə olunur. Domen administratoru hər bir işçi stansiya administratorunun sayına əlavə olunduqdan sonra bir çox hallarda cari problemlərin həlli üçün ona yaxınlaşmaq tələb olunmur.

"Məxfi" ünvanlar. Bəzən şəbəkə administratorları istifadəçilərin IP ünvanlarını gizlətməyə çalışırlar, yəni "məxfi" ünvanlara çevirirlər və bunu instrumental vasitələrin köməkliyi ilə həyata keçirirlər. Lakin belə yanaşma şəbəkənin təhlükəsizlik göstəricilərini heç də daha etibarlı etmir. Praktikadan məlumdur ki, bu şəbəkəyə məxsus istifadəçilər hər hansı ünvana elektron məktub göndərdikdə, onların hansı domenə məxsus olduğunu asanlıqla müəyyən etmək mümkündür. Yüksək səviyyədə mühafizə olunmuş şəbəkəyə daxil olmaq üçün bu məlumat kifayət etmir. Lakin əgər şəbəkə kifayət qədər mühafizə olunma yıbsa, onda bədəməl şəxs (*bədəfkar*) bu şəbəkənin daxili IP ünvanlarını asanlıqla əldə etdikdən sonra ixtiyari istifadəçinin resurslarını istifadə edə bilər. Məhz bu səbəbdən şəbəkənin daxili IP ünvanlarını məxfiləşdirməkdənsə, digər instrumental vasitələrlə şəbəkə resurslarının təhlükəsizliyini təmin etməyə və şəbəkənin giriş/çıxış sisteminin daim nəzarətdə saxlamağa çalışmaq lazımdır. Bu prosedurları həyata keçirmək üçün müxtəlif instrumental vasitələrdən istifadə edərək idarəetmə sistemini avtomatlaşdırmaq da mümkündür. Növbəti fəsillərdə biz sistem administratoru tərəfindən həyata keçirilməsi zəruri sayılan funksional-texniki tədbirlər barəsində söz açacağıq.

FƏSİL 2

İNFORMASİYANIN QORUNMASI VƏ MƏHV EDILMƏSI

İNFORMASİYANIN QORUNMASI VƏ MƏHV EDİLMƏSİ

- **Proqram vasitələrinin mühafizəsinin aktual məsələləri**
- **Proqram vasitələrinin mühafizəsinin əsas səbəbləri**
- **İcra olunan faylların əsas formaları**
- **MS Windows əməliyyat sisteminin 32 bitlik versiyasında icra olunan faylların daxili strukturunun özəllikləri**
- **Proqram təminatı üçün qeydiyyat kodlarının mühafizə sistemləri**

Fəsil 2. İNFORMASİYANIN QORUNMASI VƏ MƏHV EDILMƏSI

İnformasiyanın qorunması və məhv edilməsinin birbaşa asılı olduğu faktorlardan biri də proqram vasitələrinin mühafizə dərəcəsidir. Məhz bu səbəbdən kitabın bu fəsli kommersiya proqram təminatlarının qeyri leqal yayılmasına, icra olunan faylların əsas formatlarına, onların işləmə mexanizminə həsr olunmuşdur. Bununla yanaşı MS Windows əməliyyat sisteminin 32 bitlik versiyasında icra olunan faylların daxili strukturunun özəllikləri də geniş təhlil olunmuşdur.

2.1. Proqram vasitələrinin mühafizəsinin aktual məsələləri

Proqram təminatının yayılması üçün bir çox müxtəlif modellər vardır. Onlardan bir neçəsinin xarakterik xüsusiyyətlərinə baxaq.

Pulsuz proqramlar (*Freeware*). Proqram təminatının yayılmasının bu modelində proqramın istifadəçisi üçün heç bir ödəmə olmadığı başa düşülür. Böyük olmayan sistem proqramlar çox tez-tez bu prinsip üzrə yayılır və geniş istifadəçi dairəsinə çox xeyirli ola bilər çünki, onun istifadə edilməsi üçün heç bir ödəmə tələb olunmur. Əlbəttdə elə proqramçılar var ki, onlar öz işlərinə sevgidən bu proqramlara pulsuz əlavələr edirlər və hətta gələcəkdə bu proqramların informasiya texnologiyalarında komersiyalaşmasını düşünmədən belə çox vaxt bu işlə öz xoşuna məşğul olurlar. Çox vaxt onlar komanda yaradaraq, müxtəlif mürəkkəb proqramlar sistemini işləyib hazırlayırlar. Pulsuz proqramların əksəriyyəti müxtəlif İnternet saytlarında yerləşdirilir və bu proqramları maneəsiz yükləmək olür. Çox vaxt elə situasiyalar olur ki, orada kitabxanaların və ya proqramların istifadəsi pulsuz olur. Lakin onların işlədilməsi üçün heç də ucuz olmayan kommersiya məqsədi ilə lisenziya tələb olunur. Bəzən pulsuz proqramlar nəhəng kommersiya kompaniyaları tərəfindən hazırlanır ki, bu da bazardakı vəziyyəti möhkəmləndirmək

məqsədi güdür. Məsələn, "PDF" formatında olan sənədlər bu gün belə populyar ola bilməzdi, əgər onlara baxış üçün pulsuz proqramlar olmasaydı, bunlardan "Adobe Acrabat Reader" və "PDF" - formatının açmağa və oxumağa imkan verən onlarla digər pulsuz proqram vasitələrini göstərmək olar. Anoloji olaraq sənədlərin hazırlanması üçün yaradılmış kommersiya proqramı olan "Microsoft Word" proqramına pulsuz baxmaq üçün Microsoft korporasiyası tərəfindən "Microsoft Word Viewer" baxış proqramı yaradılıb. Pulsuz proqramların müəllifi öz yazdığı proqramlardan istifadə üçün təmənnasız kiməsə verir, o isə öz növbəsində bu proqramı daha da genişləndirərək biznes məqsədi ilə istifadə edir. Bu isə çox vaxt böyük uğurlar gətirir.

Təxmini pulsuz proqramlar. Bəzən müəlliflər hansısa düşüncə ilə öz proqramlarını kommersiya məqsədi üçün yayılmasını istəmirlər və bunun müqabilində nə isə qazanmaqdansa özlərinin mənəvi maraqlarını ödənilməsini üstün tuturlar.

Cardware – hər bir proqram istifadəçisi qeydiyyatdan keçmək istəyirsə o, proqramın müəllifinə harada yaşaması haqqında yazılı məlumat verməlidir.

Mailware – "cardware"-nin daha yeni variantıdır. İstifadəçi onun vasitəsi ilə müəllifə elektron məktubu göndərir. Cavabında müəllif istifadəçiyə qe ydiyyat kodunu təqdim edir və bunun sayəsində istifadəçi proqramla işləməyə imkan qazanır.

Donationware – proqramın istifadəsi üçün müəllif heç bir ödəmə tələb etmir. Proqramın dəstəklənməsi üçün ona çatacaq məbləği istifadəçilərə peşkəş edir.

Giftware – təxminən "donation ware" kimidir. Amma burada müəllif ona çatası pulu peşkəş etməkdən başqa, digər hədiyyələr verməyə belə hazırdır.

Vegeware – proqrama görə müəllif ödəmə əvəzinə istifadəçilərdən vegetarian xörəklər reseptini yığır.

Memorialware – Qari Kremblit (Gary Cramblit) adlı bir şəxs

yazdığı proqramı atasının xatirəsinə həsr edərək "Memorialware" kimi yaymışdır. Proqram istifadəçilər üçün pulsuzdur, lakin arzu edənlərə ata Kremblittin Memorial fonduna köməklik etməyi təklif edilir.

Reklam göstərən proqramlar (*Adware*). XX əsrin axırlarında İnternet texnologiyalarının qızğın inkişafı dövründə proqram təminatçılarının reklam şəklində nümayiş olunaraq, yayılması modeli çox populyar idi. "Ad" ingilis sözü olan "Advertisement" yəni reklamın qısaldılmış formasıdır. Bunun məğzi odur ki, proqram istehsalçıları istifadəçidən deyil, reklamçılardan öz qonorarını alırlar. İstifadəçilər proqramı yükləmək üçün hər dəfə məcburi şəkildə İnternetdə olan reklam çarxına baxmalıdırlar. Bu yanaşmada əgər proqram vasitələri İnternetdə işləmək üçün nəzərdə tutulubsa, onda özünü daha effektiv şəkildə göstərər. Lakin vaxt keçdikcə reklamların effektivliyinin aşağı düşməsi ilə əlaqədar, belə istifadəçiləri tapmaq bir qədər çətinləşdi. Buna baxmayaraq bu gün də sponsor tərəfindən maliyyələşdirilən proqram təminatları vardır. Yəni proqram təminatları onların vəsaiti hesabına yazılır və əvəzində bu proqramlar sponsorlar tərəfindən nümayiş etdirilir.

Kommersiya proqramları (*Commercial*). Çox güman ki, kommersiya proqram təminatları həm gəlir gətirmək məqsədi ilə və həm də maddi tələbləri ödəmək üçün yaradılır. Kommersiya proqramları artıq gündəlik tələbat malları kimi olub, əhali tərəfindən ona daim tələbat artır. Hər şeydən əvvəl təmiz kommersiya məqsədi ilə yazılmış proqram təminatlarının əsas prinsipi "pul – irəli" yəni istifadəçi tam ödəmə apardıqdan sonra proqramı ala bilər. Bir çox proqramlar qutu şəklində paylanılır və orada informasiya daşıyıcıları (məsələn DVD və ya kompakt-disk), proqram istifadəçiləri üçün sənədlər, qeydiyyat kartı və istehsalçı tərəfindən lazım olan bütün vasitələr qoyulur. Əlbəttə müəllif həmişə çalışır ki, təqdim etdiyi proqram üçün bütün istifadəçilərdən bunun müqabilində ödəmələri alsın. Buna nail

olmaq üçün istehsalçılar texniki metodlardan istifadə edərək, bu proqramın surətinin qeyri leqal (lisenziyasız) yayılmasının qarşısını almağa çalışırlar. Populyar texniki metodlarla müxtəlif aparat müdafiələri, hər dəfə proqram işə salınan zaman sistemdə qeydiyyat və aktivləşdirmə, İnternet vasitəsi ilə lisenziyanın yoxlanılması və s. həyata keçirilir. Lakin tam kommersiya proqram təminatının bir əsas fərqləndirici xüsusiyyəti vardır. Bu proqram təminatının alıcısı aldığı proqram məhsullarının hansı spesifik üstünlüklərə malik olduğunu yalnız istifadə edərkən tam şəkildə anlaya bilər. Burada proqram vasitəsi istifadəçinin tələblərini tam ödəməyə bilər. Dünya praktikasına əsasən inkişaf etmiş ölkələrdə əgər proqram alıcıların tələblərini tam şəkildə ödəmirsə və ya texniki xarakteristikalarında göstərilmiş imkanlardan kənara çıxma vardırsa, onda onların verdiyi məbləğ istehsalçı tərəfindən iki həftə ərzində geri qaytarılır.

İş qabiliyyətli məhdudlaşdırılmış proqramlar. Kommersiya proqramlarını reklam etmək üçün istehsalçılar öz məhsullarını tanışlıq məqsədi ilə məhdudlaşdırılmış variantda buraxırlar. Bu variantlarda işləmək, adətən məhsuldar olur və proqramın funksionallığı haqqında həqiqi təəssürat yaradır. Məhdudlaşdırılmış proqram məhsullarının bir neçə əsas tiplərini göstərmək olar.

Demoware – bu halda proqram təminatında funksional məhdudiyyətlər mövcud olur. Məsələn, hər hansı bir əməliyyat bitdikdən sonra, yekun faylı yaddaşda saxlamaq mümkün olmur və s. Belə proqramlara hərdən *"Crippleware"* – kiçildilmiş və ya kəsilmiş proqram təminatı deyilir.

Trialware – vaxta görə istifadəsi məhdudlaşdırılmış proqram yayılma metodudur. Proqramdan istifadə üçün qoyulmuş vaxtın bitməsinə qədər (məsələn yaddaşa salınandan 30 gün sonra) və ya vaxtın bitməsinin qeyd olunduğu ana qədər, məhdudlaşdırma da nəzərə alınaraq istifadə etmək mümkündür. Proqramın məhdudlaşdırılması istifadənin və ya proseslərin emalının sayına

əsasən aparıla bilər.

Nagware – istifadəçi mütəmadi olaraq, bu versiyalı proqram təminatının kommersiya tələblərinə tam cavab verməməsi haqqında xəbərdarlıq alır. Bu xəbərdarlıq dialoq pəncərəsi kimi görünə bilər və proqram isə salınan zaman ayrı-ayrı vaxtlarda əlavə yazılar kimi ekranda əks olunur. Bundan başqa müxtəlif məhdudlaşdırma kombinasiyaları da mümkündür.

Şərti pulsuz proqramlar (*Sharware*). Bu proqramı almamışdan qabaq (*try before you buy*) onu dəyərləndirməkdən ötrü, proqramın seçilmiş nişanları olan şərti pulsuz məhsulları ilə tanış olmaq lazımdır. "Share" ingilis dilindən bölüşdürmək, birgə istifadə etmək kimi tərcümə olunur. Deməli şərti pulsuz proqramları qeydiyyatdan keçirmədən və onu dəyişmədən sərbəst şəkildə yaymaq olar. Şərti pulsuz proqram təminatları və həmçinin kommersiya proqram təminatları gəlir gətirmək məqsədi ilə işlənib hazırlanır. Buna baxmayaraq potensial istifadəçiyə proqramın dəyərini ödəmədən proqramla tanış olmaq üçün müəyyən müddətə imkan verilir. Bu test dövrü qurtardıqdan sonra potensial alıcı proqramın alınması üçün qərar qəbul edir. Əgər almamaq qərarı qəbul olunursa, onda dərhal proqramdan istifadə edilməsini dayandırıb onu kompüterdən silmək lazımdır. Əks halda proqramın lisenziya müddəti bitən kimi proqram öz işini dayandıracaq. Adətən şərti pulsuz proqramlar çox kiçik ölçüdə İnternetdə yayılır. Həmçinin çox vaxt pulsuz proqramların məhdudlaşdırılmış versiyası üçün heç bir əlavə fayl tələb olunmur. Pulsuz istifadə ərəfəsində məhdudiyyətlər qoyulur ki, bunlar da kommersiya proqram məhsullarını qiymətləndirmə versiyasındakı məhdudiyyətlərə uyğun gəlir. Qiymətləndirmə dövründə dəqiq məhdudiyyətlər bir qayda olaraq hər bir konkret məhsulun istifadəsi üçün lisenziya razılaşmasında göstərilir. Şərti pulsuz proqram məhsulları olduqca populyardır. Sanballı proqram layihəçilərinin çoxu "*try before you buy*" variantını seçərək alıcıları maraqlandırmağa çalışırlar. Kommersiya proqram

təminatları ilə tanışlığın məhdudlaşdırma versiyası, "*Shareware*" proqram yayılma modelinin şərti pulsuz proqramlar ideyasının yalnız bir modifikasiyasıdır. Buna misal olaraq Microsoft korporasiyasın MS Windows Server 2003 və Visual Studio .Net versiyalarını pulsuz olaraq 120 günlük müddətə əldə etmək mümkündür. Həqiqətdə bu 120 günlük versiyanı tam hüquqlu versiyaya çevirmək üçün yeni versiyalı disk alıb müvafiq proseduranı yerinə yetirmək kifayətdir və nəticədə "klassik" şərti pulsuz proqramlardan tam versiyaya keçirmək mümkündür. Bunun üçün lisenziya kodunu düzgün qeydiyyatdan keçirmək lazımdır.

2.2 Proqram vasitələrinin mühafizəsinin əsas səbəbləri

Adətən kommersiya proqramını icazəsiz artırıb paylanmaqdan mühafizə edirlər. Proqram təminatının yerləşdiyi informasiya daşıyıcısı proqramın surətinin çıxarılmasına və icazəsiz istifadə olunmasına heç zaman imkan verməz. Distribüterin verilənlərinin surətini çıxarmaq olar, lakin sözü gedən proqram vasitəsinin digər kompüterdə düzgün işləməsi qeyri-mümkündür. Bu cür məhdudiyyətlər müxtəlif üsullarla yerinə yetirilir. Məsələn bir çox kommersiya proqramları quraşdırılan zaman onların seriya nömrələrinin yazılması tələb olunur. Bu nömrə ya qutu üzərində və ya təklif olunan proqram təminatının sənədlərinin birinə çap olunur. Məsələn, Microsoft – autentifikasiya sertifikatında qeyd edir. Həmçinin çox vaxt proqramlarla eyni zamanda işləyən istifadəçilərin sayını azaltmaq tələbatı yaranır. Yəni bir iş yerinə lisenziya almış adam eyni zamanda ikinci iş yeri yaratmaq imkanına malik olmamalıdır. Buna aparat açarlarından istifadə etməklə, menecerlərin lisenziyası və aktivləşdirmə proseduru ilə nail olmaq olar. Bir neçə proqram məhsulları üçün (məsələn oyun proqramları) informasiya daşıyıcılarını kompakt disklərdə saxlayırlar. Yəni proqramı işə salmaqdan ötrü orijinal kompakt diskdən istifadə etmək lazımdır. Əgər burada kompakt diskin

surətindən istifadə olunarsa, onda sistem işləməz, çünki bu diskin surətinin çıxarılması standart vasitələrlə mühafizə olunur.

Vaxta və saya görə məhdudlaşdırılmış proqram versiyaları qiymətləndirməkdən ötrü sayğacların düzgün işlənməsi və saxlanması vacib məsələlərdən biridir, yəni hər hansı bir adam proqramla işləyərkən özü istədiyi kimi nə saatı dəyişdirə bilsin və nə də faylı silə bilsin, əks halda burada buraxılan proqramların və işlənmiş faylların sayına nəzarət etmək mümkün olmaz.

Şərti pulsuz məhsullar funksional məhdudlaşdırılmış kommersiya proqramlarının qiymətləndirmə versiyalarından fərqli olaraq, onların qeydiyyat kodu verildikdən sonra baxılan tam versiyalı proqramın bütün funksiyalarına girmək mümkündür. Yəni pulsuz yayılan proqram versiyalarında tam versiyalı proqramın bütün funksiyaları olmalıdır. Qeydiyyat kodu olmayan proqramlarla işləyən istifadəçilər üçün elə mühafizə sistemi təşkil etmək olar ki, o yalnız düzgün qeydiyyat kodunu əldə etdikdən sonra giriş hüququ qazansın. Seriya nömrələrinin düzgünlüyü yoxlama prosedurası, qeydiyyat və aktivləşdirmə kodları elə düzülməlidirlər ki, heç kim özbaşına bu düzgün kodları dəyişə bilməsin və bu zaman kod sətirlərinin uzunluğu çox da böyük olmamalıdır. Həmçinin iş əsnasında hər hansı faylda dəyişikliklər və üzərində tədqiqat aparılmasın deyə, onu mühafizə etmək ehtiyacı yaranır.

Bütün proqram təminatının istehsalçı şirkətləri öz proqram məhsullarının və intellektual mülkiyyətlərinin qeyri-qanuni nüsxəsinin çıxarılmaması üçün mübarizə aparırlar. Qeyri-qanuni yolla proqram məhsullarının nüsxələrinin çıxarılması həm istehsalçıya və həm də istifadəçilərə ziyan vurmuş olur. Lisenziyalı proqram məhsullarını əldə edərkən istifadəçi tam əmin ola bilər ki, bu proqrama üçüncü şəxslər tərəfindən heç bir müdaxilə olunmayıb və tam funksionaldır. Lakin proqram məhsulunun mənbəyi məlum olmayan nüsxəsini əldə etdikdə istifadəçi onun tam funksionallığına əmin ola bilməz.

Proqram təminatının lisenziya müqaviləsində göstərilən istifadəçilərin sayına olan məhdudiyyət pozulduqda, yəni daha artıq sayda istifadəçi kompüterlərinə proqram yüklənildikdə, artıq lisenziya müqaviləsinin şərtləri və müəllif hüquqları pozulmuş sayılır. Lakin informasiya texnologiyalarının bu cür sürətli inkişafı dövründə belə halların qarşısını texniki vasitələrlə almaq mümkündür. Belə texniki vasitələrə misal olaraq aktivləşdirməni göstərmək olar. Aktivləşdirmə texnologiyası texniki olaraq proqram məhsulunun işlək nüsxələrinin istifadə sayını məhdudlaşdırmağa imkan yaradır. Belə yanaşma zamanı proqram məhsulunu sonsuz sayda müxtəlif kompüterlərə yazmağın qarşısı alınır. Əgər leqal proqram məhsulunun istifadəsi lisenziya müqaviləsinin bütün şərtlərinə uyğun qaydada aparılırsa, onda proqramın təkrar yazılmasına və aktivləşdirilməsinə heç bir məhdudiyyət qoyulmur.

Adətən aktivləşdirmə prosesi çox zaman tələb olunmur və proqramın tərkib hissəsi olaraq xüsusi "Aktivləşdirmə Köməkçisi" vasitəsi ilə həyata keçirilir. Aktivləşdirmə köməkçisi istifadəçidən tələb olan məlumatı istehsalçı təşkilata çatdırır və bu məlumat emal olunduqdan sonra, istehsalçı istifadəçiyə aktivləşdirmə kodunu və ya aktivləşdirmə faylının spesifik ünvanını yollayır. Aktivləşdirməni həyata keçirmək üçün proqram məhsulunun seriya nömrəsini və xüsusi kodunu (Installation ID) istehsalçı təşkilata yollamaq kifayətdir. Aktivləşdirmə kodu proqram quraşdırılması nəzərdə tutulan istifadəçinin kompüteri haqqında olan məlumat əsasında formalaşır. Aktivləşdirmə kodunun yaradılması zamanı istifadəçi haqqında şəxsi məlumatlar istifadə olunmur.

2.3 İcra olunan faylların əsas formaları

Prosessoru x86 (IBM PC XT-dən başlamış Intel 8086 prosessorlu) olan fərdi kompüterlər yarandığı müddət ərzində bir neçə ikili fayl forması dəyişib. Əməliyyat sistemi DOS (Disk Operating Sistem)

iki əsas faylla: "com" və "exe" – ilə idarə olunub. "com" faylı operativ yaddaşda əlavə sazlamalar olmadan düzgün yüklənir və onların ölçüləri 64 Kb-dan böyük olmayır. Başlıqdan ibarət olan "exe" faylının isə ölçüyə görə çox ciddi məhdudlaşdırılması olmayır. Bu fayl özündə lazımi informasiyaları birləşdirərək və onun vasitəsi ilə proqramın yaddaşa düzgün yüklənməsinə xidmət edir. "DOS" əməliyyat sistemində "exe" fayllarının başlığı "MZ" və ya "ZM" simvolları ilə başlayır və onu "MZ Header" (MZ-başlıq) adlandırırlar. "MZ" hərifləri Marka Zbikowski-nin soyadı olub, bu proqramın yaradıcısının şərəfinə belə adlanır. Hal-hazırda bütün istifadə olunan fayllar "MZ" başlığında saxlanılır. MS Windows əməliyyat sisteminin 16 bitli versiyasının meydana gəlməsi ilə əlaqədar olaraq faylların geniş formatda istifadə olunmasına ehtiyac yarandı. MS Windows əməliyyat sistemində kitabxanaların birləşdirilməsinin dinamik dəstəklənməsi yerinə yetirilib (Dynamic Link Library - DLL) buna görə də yeni format, göndərilən ixrac (export) cədvəlləri (DLL-də yerləşən və digər modullar üçün yarayan) və qəbul olunan (İmport) funksiyaları, (xarici kitabxanalarında yerləşən) yaddaşa salma imkanına malik olmalıdır. Bundan əlavə MS Windows əməliyyat sistemində ikili dialoqların yazılması və s. geniş istifadə olunur, bu yaxşı olardı ki, icra olunan faylların daxilində saxlansın. Format yaradılan zaman, o momentə aktual olan tələblərin hamısı nəzərə alınır və "New Executable" - yeni yaradılmış fayl adını alır. Belə faylın başlığı "NE" simvolu ilə başlayır. MS Windows əməliyyat sisteminin virtual qurğusunda (Virtual Device Driver - VxD) darayverləri saxlamaq üçün "Linear Executable" (LE, xətti icra olunan fayl) formatı tətbiq olunur. Onu modifikasiya olunmuş "Linear Executable" (LX) adlandırırlar, OS/2 əməliyyat sisteminin 2.0 versiyasından başlayaraq və icra olunan faylıların saxlanılmasında və ya qorunmasında geniş istifadə olunur. MS Windows NT Server 4.0 əməliyyat sisteminin yaradılması ilə əlaqədar Microsoft korporasiyası tərəfindən "Portable Executable" (PE, daşınan icra

olunan fayl) formatı hazırlandı. Daha dəqiq Unix əməliyyat sistemində istifadə olunan "COFF" (Common Object File Format) obyekt formatlı faylların oxşarından götürülərək, lazım olan şəkildə işləyib hazırlanmışdır. Daşınan sözü onu göstərir ki, eyni faylın formatını bütün 32 bitli əməliyyat sistemi olan Microsoft x86 platformasında və MS Windows NT Server 4.0 əməliyyat sisteminin digər platformalarında (MIPS, Alph və Power PC) istifadə etmək mümkündür. Müasir MS Windows əməliyyat sisteminin bütün versiyaları üçün bu format əsas sayılır və ona görə də kitabda buna böyük diqqət yetiriləcəkdir.

2.4 MS Windows əməliyyat sisteminin 32 bitlik versiyasında icra olunan faylların daxili strukturunun özəllikləri

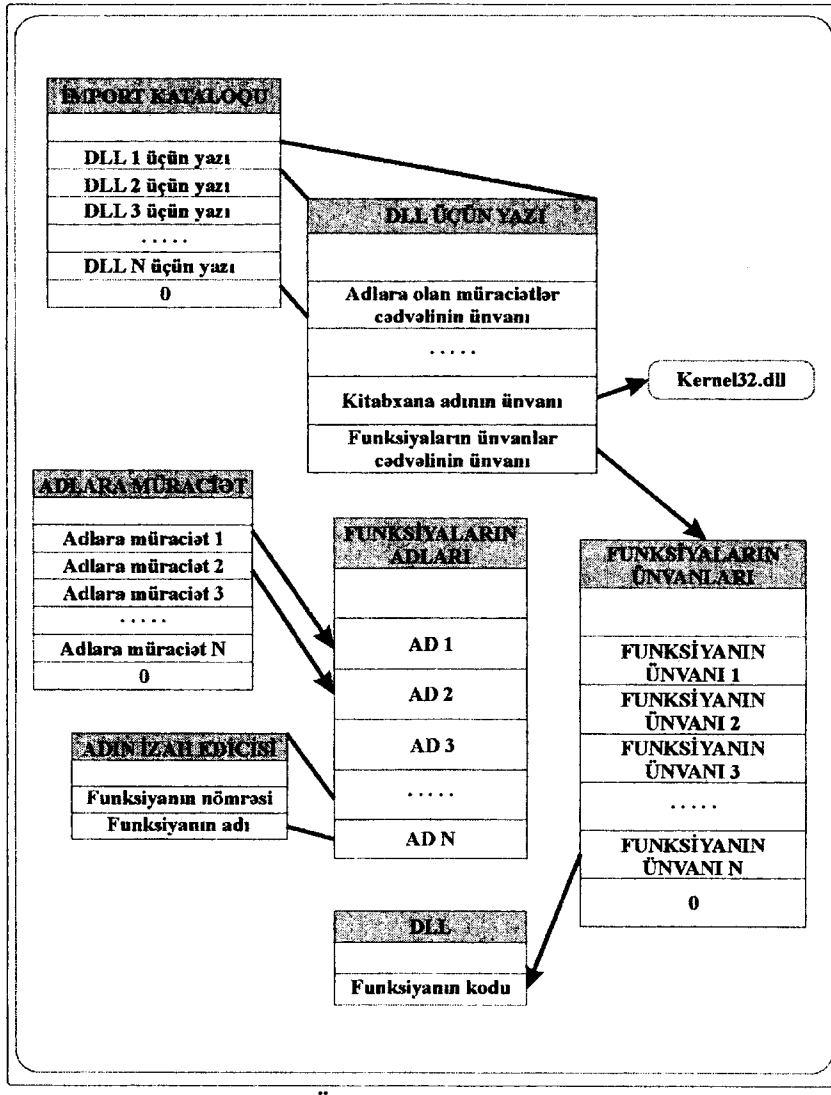
"Portable Executable" (PE) formatının detallarının hamısına deyil, yalnız mühafizə prosesində qarşılıqlı təsirə məruz qalan hissələrini qeyd edək. "PE" faylının daxilində çox böyük sayda müxtəlif sahələr və cədvəllər yerləşir. Bu sahələrdən biri giriş nöqtəsini (Entry Point), proqramın yerini və oradan da proqram yaddaşa verildikdən sonra idarə olunmaq üçün lazımi yerə göndərilməsini təyin edir. "DLL" (Dynamic Link Library) tipli fayıllarda idarə etmə zamanı həm kitabxananın yaddaşa yüklənilməsi həm də silinməsi zamanı giriş nöqtəsinə müraciət edir. Adətən icra olunan fayllar bir neçə bölmədən ibarət olur (daha dəqiq "PE" başlığında bu bölmələrin sayı göstərilmişdir). Rabitə redaktoru olan "Linker" bir qayda olaraq eyni tipli informasiyaları bir bölmədə birləşdirir. Tipik icra olunan fayl özündə bölmənin kodunu, yəni statik və dinamik verilənləri və bölmə resurslarını saxlayır. Hər bir seksiya özünün adına, ölçüsünə, faylda və yaddaşda vəziyyətinə, həmçinin dəst atributlarına görə (ikili bayraq) kodu və ya bölmədə verilənlərə əsasən müəyyənləşdirilir. Proqram işi yerinə yetirərkən bölmənin koduna şəxsi komandasını yerləşdirir. Bu bölmədə olan atributlar kodun yerinə yetirilməsini və istifadə olunmasını

qadağan edir. Proqram yaddaşa yazıldıqdan sonra statik verilənlər dəyişmir, buna görə də adətən statik verilənlərin bölməsi üçün yazılışı icazə verən atribut quraşdırılmır. Proqram yerinə yetirilən anda bu bölməyə yazma əməliyyatı aparılmasına cəhd edilərsə bu istisna hala gətirib çıxarır (*exception*). Bölmə atributunun dinamik verilənlərini isə əksinə olaraq ona yazılmasına icazə verir. Yuxarıda icra olunan faylların tutumlarının bölmələr üzrə paylanması imkanlarından birinin sxemi verilmiş və "PE" faylı yaradan proqram vəsaitinin hər biri hansı informasiyanın, hansı bölmədə olunmasını həll edir. Hətta bütün proqramlar bir bölmədə yerləşə bilər və bu onların tam iş qabiliyyətli olmasına xələl gətirməz. "PE" faylının başlığında bölmə haqqında yazıdan əlavə xüsusi kataloq (*PE Directory*) olur, hansı ki, orada proqramın yaddaşa düzgün yüklənməsindən ötrü ölçülər və xidmət strukturu göstərir. Bu strukturlar proqram resurslarının hansı yerdə saxlanmasını, ünvanların göndərilmə funksiyalarını necə axtarmağı, ünvanların alınmasına göndərilmək üçün hazırlığı və s. təyin edir.

Qəbuletmə funksiyası - bu modullarda digər icra olunan funksiyalar yerləşir, onlar yalnız iş vaxtı istifadə olunaraq, ancaq alınan idxal (import) cədvəllərin ardıcıllığını qeyd edir. Bu öz aralarında əlaqəsi olan dörd cədvəldən ibarətdir:

- *idxal kataloqu* (Import Directory Table - IDT);
- *funksiyaların adına göndərilən cədvəl* (Lookup Table);
- *qısa adların cədvəli* (hint-Name Table);
- *idxal ünvanlar cədvəli* (Import Address Table - IAT).

Qəbul etmə cədvəlinin vəzifəsi, qəbul edilən funksiyaların bütün göstəricilərini və ya qiymətlərini ünvanlar cədvəlində düzgün doldurmaqdan ibarətdir. Bu qiymətlərdən hər biri özü-özlüyündə xarici kitabxana olaraq, prosessorun ünvan fəzasına yüklədikdən sonra, təyin olunmuş ünvan funksiyasını daşıyır (şəkil 2.1). "PE" (Portable Executable) faylları daha çox müxtəlif cədvəllər və atributlar tutumuna malik olurlar.



Şəkil 2.1 Ünvanların alınması cədvəli

2.5 Proqram təminatı üçün qeydiyyat kodlarının mühafizə sistemləri

Əldə olunmuş materialların və ya sənədlərin qeydiyyatdan keçirilmə prosedurası dünya praktikasında olduqca çoxdan

mövcuddur. Alış veriş qurtardıqdan sonra alıcı özü haqqında qeydiyyat kartına məlumatlar yazaraq onu istehsalçıya göndərir. Bu minvalla alıcı qeydiyyatdan keçmiş istifadəçiyə çevrilir. İstehsalçı müştəriləri haqqında olan bütün statistik məlumatları özündə qeyd edərək, onlara lazım olan bütün texniki və zəmanət xidmətlərini həyata keçirir. Qeydiyyat kartları müxtəlif "qutu" proqram məhsulları ilə birlikdə və həmçinin son zamanlar bu qeydiyyat məlumatları İnternet vasitəsilə də yayılır.

Əgər istifadəçinin adı unikal deyilsə, onda göndərilən hər bir məhsulu bir neçə təkrar olunmayan rəqəmlərlə, necə deyərlər seriya nömrələri ilə əlaqələndirmək lazımdır. Bu nömrə istifadəçi tərəfindən qeydiyyat kartı doldurulan zaman göstərilir və gələcəkdə istehsalçıya müraciət olunduğu vaxt istifadə olunur. Proqram təminatına əlavələrdə isə seriya nömrələri köməkçi funksiyasını yerinə yetirə bilər və qeyri leqal surət çıxarma ilə məhdudlaşar.

Proqram vasitəsinin surəti qeyri-qanuni çıxarılarsa, ondan istifadə etmək qeyri-mümkündür, çünki proqram quraşdırılan zaman seriya nömrələrinin düzgün yazılmasını tələb edəcək. Seriya nömrələrinin yayılması bu nömrələrdən qeyri-qanuni istifadə edənləri tapmağa və cəzalandırmağa şərait yaradır. Bir neçə proqram quraşdırıldıqdan sonra proqramın bütün funksiyalarından istifadə etmək üçün istifadəçi daha bir proseduranı yerinə yetirməlidir, qeydiyyatdan və ya Microsoft aktivləşdirməsindən keçməlidir. Qeydiyyatdan keçmə prosedurası onun üçün lazımdır ki, istehsalçılar lisenziyalı proqram istifadəçiləri haqqında tam məlumata malik olsunlar və hər hansı bir çatışmamazlıq meydana çıxdıqda istifadəçilər istehsalçının dəstək xidmətindən yararlana bilsinlər.

Tələblər və siniflərə ayrılma. Proqram özündə bir neçə mexanizmi birləşdirməlidir ki, onun vasitəsi ilə istifadəçinin göstərdiyi seriya və ya qeydiyyat (aktivləşdirmə kodu) nömrəsinin düzgünlüyünü yoxlamaq mümkün olsun. Göstərilmiş seriya

kodlarının düzgünlüyü və tətbiqi imkanı həmişə proqram təminatçılarının əlində olmalıdır. Bədəməl şəxs bir neçə baytı dəyişdirdikdən sonra ilk baxışdan elə görünür ki, o düzgün qeydiyyatdan keçərək proqramı aktivləşdirib, lakin həqiqətdə bu belə deyil. Lazım olan kod fraqmentlərinə və ya verilənlərə girişi olan şifrlənmiş dayanaqlı alqoritmlər qeydiyyat kodundan istifadə edərək şifrləmə açarının hesablanmasından sonra bu proqramı leqal istifadəçi işlədə bilər. Yəni qeydiyyat kodunu bilmədən proqramın tam versiyasını almaq mümkün deyil. Bu funksionallığı "ASProtect" (ASPask software) proqramı təmin edir. Generasiyanın müxtəlif metodlarını və kodların yoxlanılmasının bir neçə meyarını təyin etmək olar:

- kodu istifadəçinin adi ilə və ya kompüterin xarakteristikası ilə əlaqələndirmək imkanı;
- öhdədə yalnız alqoritm yoxlanması olduqda hər hansı bir düzgün kodun hesablanmasının qeyri-mümkün olması;
- bir istifadəçinin yoxlama alqoritmini və düzgün kodunu bilərək digər istifadəçinin kodunun hesablamaq mümkün deyil;
- qeydiyyat kodunun bloklaşdırılmasında (qara siyahıya salınması) proqramın açılmasının qeyri-mümkünlüyü (şifrləmə açarının alınması);
- sətir açarının uzunluğu.

Qeydiyyat kodlarının yoxlanma metodları - bütün kodların düzgünlüyünün yoxlanma metodlarını şərti olaraq 3 kateqoriyaya bölmək olar:

- alqoritmik, "qara qutu" prinsipinə əsaslanaraq;
- alqoritmik, çətin riyazi məsələlərə əsaslanaraq;
- cədvəll.

"Qara qutu" - bütün alqoritmik yoxlanma metodları istifadəçinin kodu ilə və ya onun kompüteri haqqında məlumatlarla əlaqə saxlamağa imkan verir. Beləliklə, leqal olan proqramların surətlərinin çıxarılması bir qədər mürəkkəbləşir.

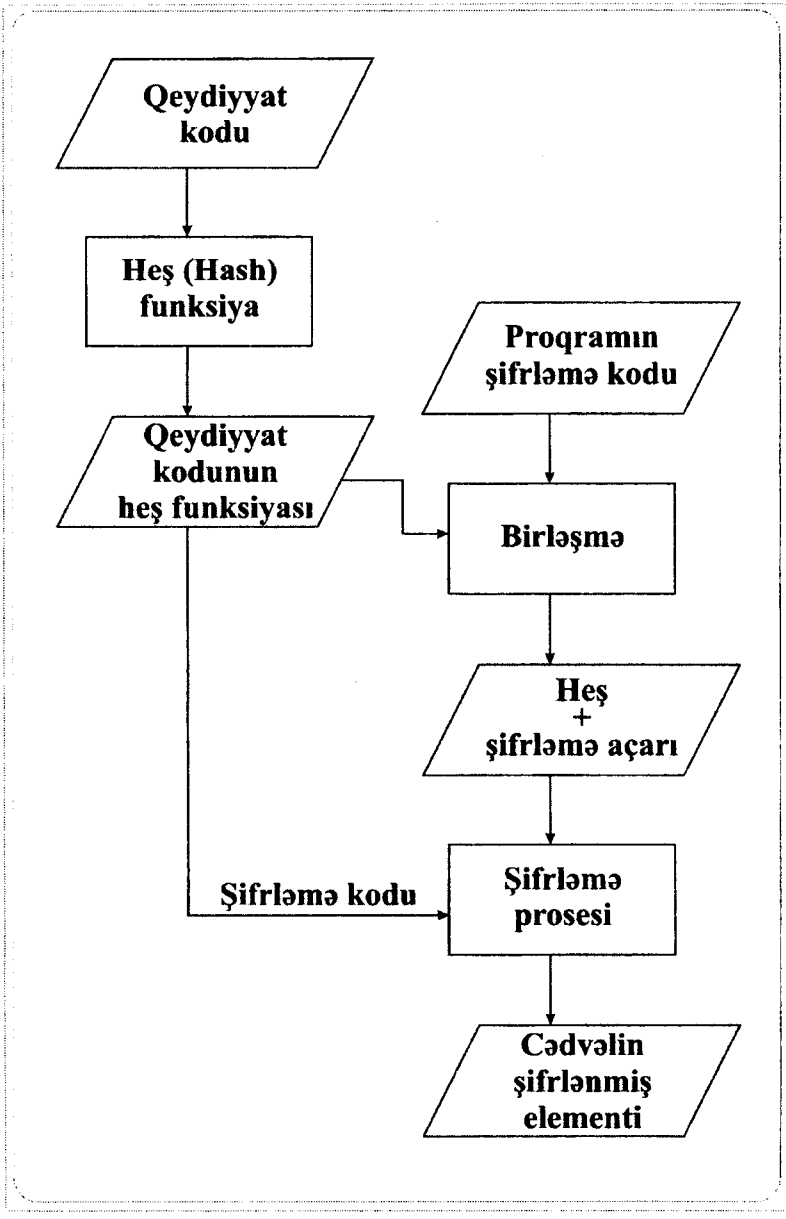
Qara qutudan istifadə edən zaman proqram təminatçıları alqoritm yoxlamalarını qarışdırmağa çalışırlar ki, ona müraciət etmək və onu başa düşmək çətinləşsin. Belə yanaşma demək olar ki, bütün istehsalçılar tərəfindən istifadə olunur. Bunu yalnız sərişləsiz proqram təminatçıları etmirlər. Məsələn, "FLEXlm" tərəfindən müdafiə olunan bir çox proqram məhsulların saxta lisenziyasına rast gəlinir. Amma "FLEXlm" 7.2 versiyasından başlayaraq bu təhlükə demək olar ki, yox dərəcəsindədir və bu lisenziya elliptik əyrilər əsasında qorunur ki, hətta qəliz riyazi məsələlərin tətbiqi ilə də bu lisenziya saxtalaşdırıla bilməz. Əgər yoxlama proseduası yazılarkən heç bir ciddi səhvə yol verilməyibsə, ondan düzgün kod almaq qeyri-mümkündür. Lakin proqrama müdaxilə edə bilən hər bir şəxs əgər heç olmasa düzgün kodlardan birini bilərsə, onda o, yoxlama proseduasına müraciət edərək yeni kodları ala bilər.

Cədvəl metodu - cədvəl metodunda verilmiş qeydiyyat kodlarının sayı generasiya olunur (mümkün istifadəçilərin sayı ilə) və bu kodlar əsasında proqramda cədvəllər saxlanılır. Əlbəttə kodlar istifadəçinin adından və ya sistemin xarakteristikasından asılı ola bilməzlər. Çünki, birinci istifadəçilər yaranana qədər onlar generasiya olunur. Ən sadə üsul – proqramda hər bir kodun kriptoqrafik hesablamasının nəticəsi olan "heş funksiyasını" saxlayır. Bununla açarın düzgünlüyünü yoxlamaq onun heş funksiyasını hesabladıqdan sonra asanlaşır, heş funksiyasının qiymətlərini bilmədikdə, onda açarı hesablamaq praktik olaraq qeyri-mümkündür. Əgər qeydiyyat kodlarının bir hissəsi statistik olarsa, onlardan proqram şifrləmək üçün istifadə etmək olar. Belə yanaşmada bloklaşdırılmış kodun məhv edilməsi çox asan olur. Amma bunun qarşısını almaqdan ötrü proqramın daxilində saxlanılan heş funksiyası cədvələ əlavə olunmalıdır və ya heşin düzgünlüyünün yoxlanılması dayandırılmalıdır. Ona görə də proqram məhsulunun hər bir yeni versiyası üçün şifrləmə açarının təsadüfü yolla seçilməsi məqsədə uyğundur. Əlbəttə hər bir yazı

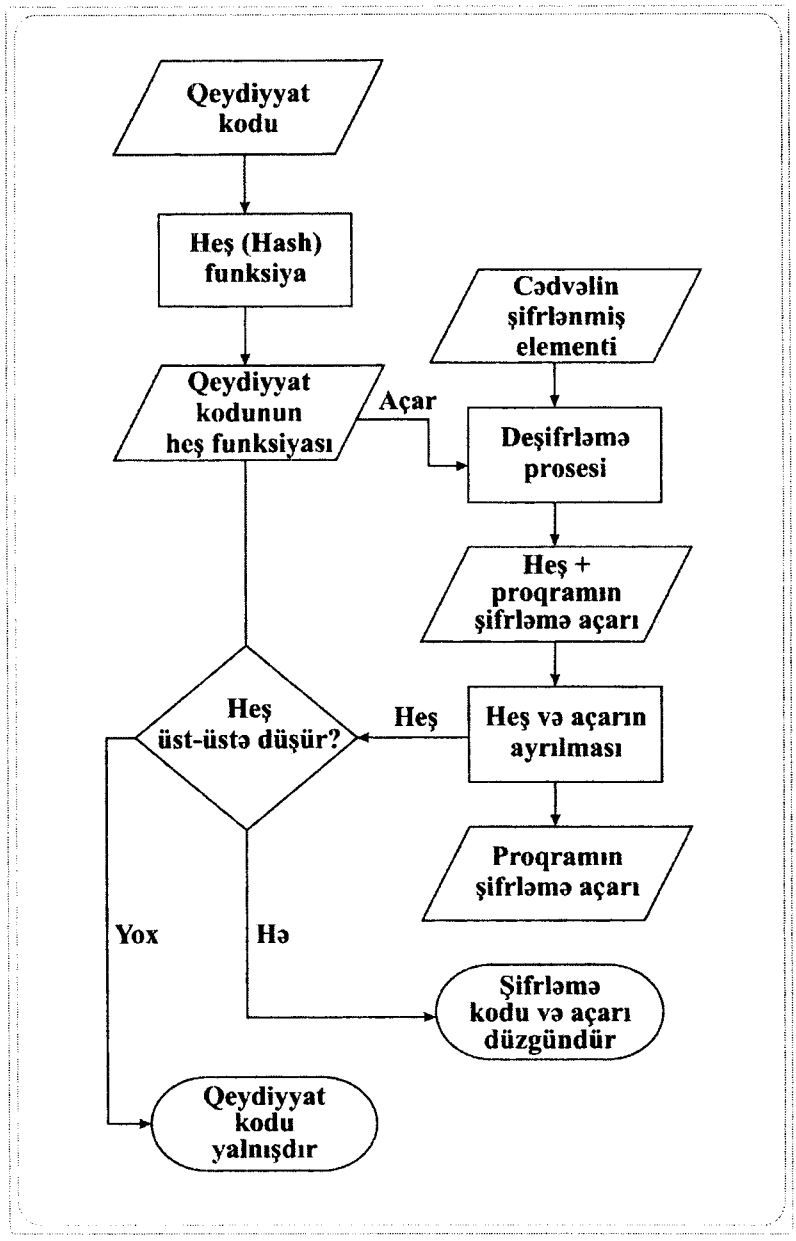
özündə bir neçə nəzarət informasiyası saxlamalıdır ki, açılışın düzgünlüyünü qiymətləndirmək mümkün olsun. Şəkil 2.2-də yazının formalaşmasında istifadə olunan alqoritmik blok sxemi göstərilmişdir və bu da ayrı-ayrı qeydiyyat kodlarına uyğun gəlir. Şəkil 2.3-də əks alqoritm göstərilmişdir və bu alqoritmin vasitəsi ilə qeydiyyat kodunun düzgünlüyünü yoxlamaq, həm də proqramın şifrləmə açarını əldə etmək mümkündür. Bu zaman hər bir qeydiyyat kodu digərlərindən heç cür asılı olmur, amma proqramın şifrləmə açarını hesablamaq çox asan olur.

Kodu bloklaşdırmaq üçün cədvəldə ona uyğun olan yazını silmək lazımdır. Əgər iş əsnasında istifadəçilərin sayı generasiya olunmuş qeydiyyat kodlarının sayından çox olarsa, onda cədvəli hər hansı arzu olunan ölçüyə qədər artırmaq olar. Yeni əlavə olunmuş qeydiyyat kodlarının sahibləri, proqramın köhnə versiyası olan lisenziyalı istifadəçilər kimi tanınmırlar. Əvvəl yaradılan kodların düzgünlüyünün yoxlanma metodlarının müsbət cəhətləri ilə bərabər mənfi cəhətləri də vardır. Belə ki, "qara qutu" müqayisədə çox sadə olaraq, iş zamanı istifadəçilərin adına olan qısa kodlardan istifadə etməyə şərait yaradır. Bu cür yanaşmada həmişə açarların generasiyasını yaratmaq imkanı olur. Dayanaqlı kriptoqrafiyaya əsaslanan metodlar iş zamanı uzun kod sətirləri tələb edir ki, bu da onun müstəqil işləməsi üçün çox çətin olur.

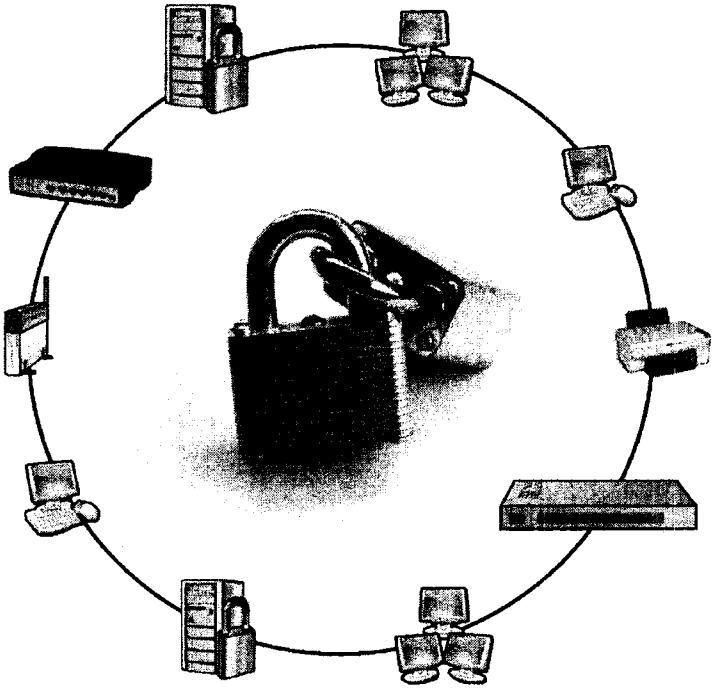
Bundan əlavə alqoritmlərin çoxu digər istifadəçilər tərəfindən özbaşına istismar olunmasın deyə patentləşdirilir. Yalnız cədvəl metodları qeydiyyat kodlarına tam bloklaşdırma imkanı verir, lakin kodun istifadəçinin adına yazılmasına imkan vermir. Bundan əlavə əgər istifadəçilərin sayı həddindən artıq çoxdursa, onda cədvəlin tutumunu da ona uyğun artırmaq olar. Ümumiyyətlə açarların generasiya metodunun seçilməsində, hər bir konkret hal üçün proqram məhsulunun xassələrinə əsaslanaraq, bazarın potensial xarakteristikasına və s. baxmaq lazımdır.



Şəkil 2.2 Açarlar cədvəlində yazıların formalaşdırılması



Şəkil 2.3 Qeydiyyat kodunun yoxlanılması



FƏSİL 3

KORPORATİV ŞƏBƏKƏLƏRİN LAYİHƏLƏNDİRİLMƏ MƏRHƏLƏSİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİNİN QİYMƏTLƏNDİRİLMƏSİ

KORPORATİV ŞƏBƏKƏLƏRİN LAYİHƏLƏNDİRİLMƏ MƏRHƏLƏSİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİNİN QİYMƏTLƏNDİRİLMƏSİ

- Təhlükələrin korporativ şəbəkələrdə reallaşma texnologiyasının analizi
- Korporativ şəbəkənin informasiya təhlükəsizliyinin qiymətləndirilməsi üçün uyğun etibarlılıq modelinin seçilməsi
- Layihələndirilmə mərhələsində korporativ şəbəkənin informasiya təhlükəsizliyinin qiymətləndirilməsi metodu
- Korporativ şəbəkənin informasiya təhlükəsizliyinin qiymətləndirilməsi üçün qeyri-səlis model

Fəsil 3. KORPORATİV ŞƏBƏKƏLƏRİN LAYİHƏLƏNDİRİLMƏ MƏRHƏLƏSİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİNİN QİYMƏTLƏNDİRİLMƏSİ

3.1. Təhlükələrin korporativ şəbəkələrdə reallaşma texnologiyasının analizi

Təhlükəsiz korporativ şəbəkələrin layihələndirilməsində potensial mümkün olan təhlükələrin analizi ilk və vacib mərhələlərdəndir. Təhlükə dedikdə, kiminsə maraqlarının pozulmasına gətirib çıxaran potensial mümkün ola bilən hadisə, hərəkət (təsir), proses və ya hallar başa düşülür. Hücum isə - bədəməl şəxsin sistemə daxil olub və bu sistemdən bəd məqsədlər üçün istifadə etmək hadisəsidir. Bədəməl şəxsin açıq şəbəkəyə qoşulmuş korporativ şəbəkələrə hücumunun əsas məqsədi və niyyəti bu sistemlərin informasiya və şəbəkə resurslarına giriş əldə etməkdən ibarətdir. Korporativ şəbəkələrdə informasiya resurslarına aid olan verilənlər bazasını, fayl serverlərini və s. göstərmək olar. Şəbəkə resursları dedikdə isə müxtəlif şəbəkə servisləri, məsələn: telnet, elektron poçt və s. başa düşülür.

Korporativ şəbəkələrin fərqli cəhətlərindən biri də odur ki, burada həm aparat təminatı (kompüterlər, serverlər, routerlər), həm də informasiya resursları paylanmış şəkildə olur. Bu səbəbdən iki tip hücumu qeyd etmək olar. Birinci tip hücumda bədəməl şəxs öz hücumlarını məhz korporativ şəbəkənin infrastrukturu və protokollarına yönəldir və bu zaman şəbəkənin infrastrukturu və protokollarında olan boşluqlardan istifadə etməklə öz məqsədinə çatmış olur. İkinci halda isə hücumlar telekommunikasiya servislərində olan boşluqlardan istifadə etməklə, məhz onların sıradan çıxardılmasına yönəldilir.

Bir qayda olaraq hücumlar aşağıdakı altı əsas sinifə ayrılırlar:

1. *Təsir xarakterinə görə* hücumlar iki hissəyə ayrılırlar: passiv (rabitə kanallarının gizli qulaq asılması, klaviaturadan daxil olan informasiyanın ələ keçirilməsi) və aktiv (korporativ şəbəkənin və ya İnternetin iki istifadəçisinin arasında olan informasiya mübadiləsində verilənlərin dəyişdirilməsi);

2. *Təsir məqsədinə görə* yəni informasiyanın və informasiya resurslarının əsas xassələrinin pozulmasından asılı olaraq onların konfidensiallığının, tamlığının və həmçinin bütün sistemin əlyetənliyinin və ya onların ayrı-ayrı servislərinin (məsələn xidmətdən imtina tipli hücumlar) pozulmasıdır;

3. *Təsirin başlama şərtlərinə görə* hücumlar qeyri şərtsiz və ya hücum edilən obyektdən hər hansı bır sorğunu göndərilməsi zamanı və yaxud hücum edilən obyektə gözlənilən hadisənin baş verməsi halında aktivləşə bilərlər;

4. *Hücum edilən obyekt ilə əks əlaqənin olmasına görə* hücumları əks əlaqəli və ya əks əlaqəsiz (biristiqamətli) kimi fərqləndirirlər;

5. *Hücum subyektinin hücum edilən obyektə nəzərən yerləşməsinə görə* hücumlar seqment daxili və seqmentlər arası olurlar;

6. *OSI açıq sistemlərin qarşılıqlı etalon modelinə görə* təsirin baş verməsi. Hücum, etalon modelinin - fiziki, kanal, şəbəkə, nəqliyyat, seans, təqdim etmə və tətbiqi səviyyələrinin yeddisində də reallaşa bilər.

Müasir informasiya texnologiyaları dünyasında aktual sayılan korporativ şəbəkələrə olan hücumların bir çox tipik sxemləri mövcuddur, bunlardan bəziləri ilə tanış olaq:

1. *Şəbəkə trafikinin analizi.* Bu tip hücumum imkanları aşağıdakılardır:

• Sistemdə baş verən hadisələrin, tam surətini əldə etmək və bunun nəticəsi kimi bədəməl şəxs əvvəlcədən verdiyi müvafiq komandalar hesabına məsələn, sistemdə tam hüquqlu istifadəçi

statusu ala bilər və ya öz imkanlarını sistem daxilində artırmaq hüququnu əldə edər

• Şəbəkə əməliyyat sisteminin komponentlərinin qarşılıqlı mübadiləsi nəticəsində ötürülən verilənlər selinin ələ keçirilməsi - məxfi məlumatın əldə olunması, əvəz olunması və dəyişdirilməsi (məsələn, şifrləməyə nəzərdə tutulmayan "FTP" və "Telnet" protokolları əsasında uzaqlaşdırılmış hostlara daxil olmaq üçün nəzərdə tutulan istifadəçilərin statik parolları) və s.

Təsir xarakterinə görə bu tip hücumlar passiv hücumlar sinfinə aiddir. Əks əlaqəsiz hücumları reallaşdıran zaman, adətən OSI modelinin kanal səviyyəsində şəbəkənin bir seqmenti daxilində konfidensiallığın pozulmasına səbəb olur. Misal olaraq korporativ şəbəkələrin əsasını təşkil edən "Ethernet" şəbəkəsində verilənlərin ələ keçirilmə hücumunun texnologiyasını nəzərdən keçirək. Məlum olduğu kimi CSMA/CD (Ethernet protokolu) protokolu əsasında verilənlərin mübadiləsi korporativ şəbəkənin bir seqmentinin daxilində bütün istifadəçilərə paketlərin göndərilməsini nəzərdə tutur. Paketin başlığı qəbul edəcək mənbənin ünvanını özündə saxlayır. Nəzərdə tutulur ki, ancaq müvafiq ünvanı olan mənbə paket qəbul edə bilər. Əgər korporativ şəbəkənin hər hansı bir fərdi kompüteri paketlərin başlıqlarından asılı olmayaraq hamısını qəbul edirsə, onda deyirlər ki bu mənbə qarışıq (promiscuous) rejimində işləyir. Adi açıq şəbəkələrdə parollar haqqında məlumat sadə mətn şəkilində ötürülür (şəbəkədə parollar açıq şəkildə TCP/IP-23-cü port, POP3-110-cu port, FTP – 21-ci port, UDP-1024-2000-ci port, Poppasswd – 106-cı portunda reallaşır). Belə vəziyyətdə bədəməl şəxs üçün şəbəkənin ixtiyari bir kompüterini əvvəlcədən özünə *"root"* hüququ müəyyən edərək qarışıq rejimə keçirmək heçdə çətin olmur və rabitə kanallarından keçən paketləri analiz etməklə korporativ şəbəkənin digər kompüterlərinin parollarını əldə edir.

Ötürülmə zamanı verilənlərin ələ keçirilməsində ən çox istifadə olunan metodlardan biri şəbəkə vasitələrinin analizatoru

və ya "*sniffer*" adlanan informasiya selinin yoxlama vasitələridir. Hal-hazırda çoxlu sayda "sniffer-proqramlar" mövcuddur. Misal üçün, Sun Microsystems korporasiyasının Solaris 10 əməliyyat sistemində işləyən "Esnifff.c" proqramını göstərmək olar. Bu proqram "Telnet", "FTP", "rlogin" sessiyasının ilk 300 baytını ələ keçirərək asanlıqla parolu və identifikatorunu müəyyən edir. Bu proqramdan başqa, Lunix əməliyyat sistemi üçün nəzərdə tutulan "sniffer" proqram – "Linsniffer", Windows NT əməliyyat sistemi üçün – "BUTTSniffer", "LANAnalyzer", "PacketBoy", MS Windows XP və ya Windows 9x əməliyyat sistemi üçün – "Lan Trace", "Shomiti Surveyor" proqramları da mövcuddur. Sniffer proqramları silsiləsinə aid ən son və texniki imkanları geniş olan proqramlara misal olaraq "IP-Watcher", "Expert Sniffer" və Network General şirkətinin məhsulu olan "Sniffer Network Analyzer" proqramını göstərmək olar. Trafik analizatorları OSI etalon modelinin bütün səviyyələrində işləmə qabiliyyətinə malikdirlər və 250-dən artıq protokolu deşifrələyə bilərlər.

2. *Korporativ şəbəkənin etibarlı obyektinin və ya subyektinin dəyişdirilməsi* və rabitə kanalları vasitəsi ilə onun adından şəxsi giriş hüquqlarının mənimsənilməsi verilənlərinin yayımlanmasıdır. Etibarlı obyekt dedikdə biz serverə leqal şəkildə qoşulmuş stansiyanı nəzərdə tuturuq. Bu tip hücum aktiv hücumlar siyahısına aiddir, əsasən informasiyanın konfidensiallığı və tamlığının pozulmasına yönəlir. Sözü gedən hücum həm daxili, həm də xarici seqmentlərdə özünü göstərə bilər, həmçinin şəbəkə və nəqliyyat səviyyələrində hücum obyekti ilə əks əlaqəli və ya əlaqəsiz reallaşa bilər. Bu tip hücumların ən çox yayılan variantı impersonasiyadır (qoşulmanın imitasiyasıdır, spoofing). İmpersonasiya zamanı bədəməl şəxsin qovşağı imitasiya etdiyi qovşağın üstünlüklərindən istifadə etmək üçün özünü digər qovşaq kimi qələmə verir. Şəkil 3.1-də əks əlaqəsiz TCP-qoşulmanın imitasiyasından istifadə etməklə hücum sxemi verilmişdir.

a) Bədəməl şəxs "A" qovşağından ISN(A) verilənlər ardıcıllığını əldə etmək naminə "A" qovşağı ilə əlaqə yaratmaq üçün bir neçə sınaq cəhdlər edir. "A" qovşağından SYN seqmentini əldə edən kimi, bədəməl şəxs "RST" bayraqlı seqmenti göndərməklə yaradılmış qoşulmanı yarıya endirir. Alınan ISN(A) verilənlərini analiz edərək, bədəməl şəxs bu verilənlərin formalaşma qanunauyğunluğunu təyin edir.

b) Bədəməl şəxs "A" qovşağına "B" qovşağı adından SYN seqmentini göndərir.

c) "A" qovşağı "B" qovşağına öz SYN seqmenti ilə cavab verərək "B" qovşağının SYN seqmentini təsdiqləyir və bu qoşulma üçün ISN(A) verilənlərini göstərir. Lakin, bədəməl şəxs bu seqmenti görmür. Əvvəlcədən alınmış məlumatlar əsasında bədəməl şəxs ISN(A) verilənlərini təyin edir və həm ISN(A)+1 təsdiqini özündə saxlayır, həm də tətbiqi proses üçün verilənləri "B" qovşağı adından "A" qovşağına göndərir. Bu seqmenti alan "A" qovşağı, "B" qovşağı ilə qoşulmanın tam hesab edir və alınan verilənləri tətbiqi prosesə ötürür. Beləliklə bu addımlardan sonra hücum tam reallaşır. Artıq bədəməl şəxs verilənləri komanda şəklində daxil edə bilər. "A" qovşağı isə bütün bu komandaları yerinə yetirəcək çünki, onlar əvvəlcədən etibar olunan "B" qovşağından gəlmiş olurlar.

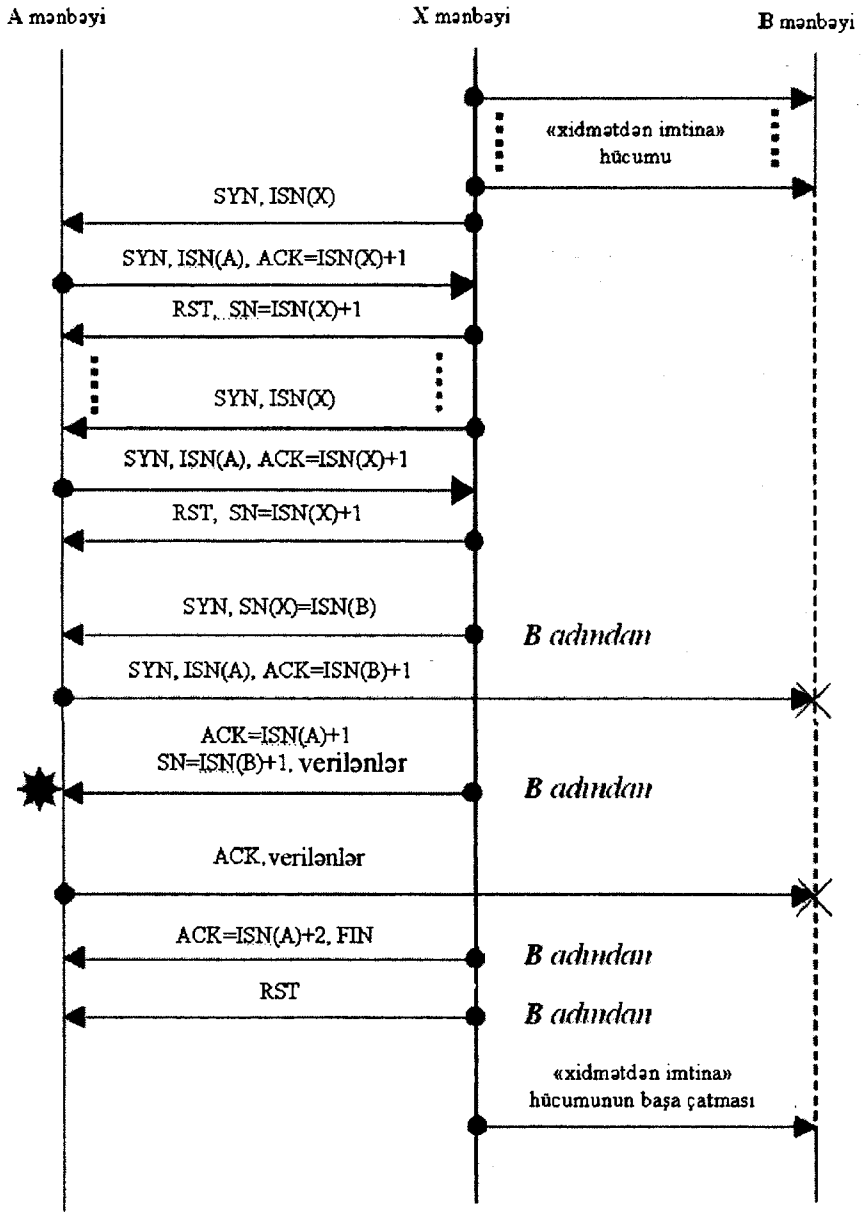
d) "A" qovşağı "B" qovşağına verilənlərin qəbul etdiyi barədə və həmçinin şəxsi məlumatını göndərir. Lakin bədəməl şəxs bu seqmentləri almayacaq, amma bu məlumat bədəməl şəxsi heç maraqlandırmır (qarşıya qoyulan məsələnin şərtinə əsasən). Bədəməl şəxs bağlantını konkret şəkildə kəsmək üçün ixtiyarı (ACK SN=ISN(A)+2) oktedinin qəbulunu təsdiq edən paketi "B" qovşağı adından "A" qovşağına göndərir. Bunun ardıca isə "FIN" bayraqlı seqmenti göndərir.

Beləliklə, korporativ şəbəkədə "X" (yəni "B", əvəzlənmiş) qovşağından "A" qovşağına qədər olan məlumat ötürmə kanalı tam şəkildə bağlanır. B ağlantının tam kəsilməsinə əmin olmaq

üçün bədəməl şəxs "FIN" seqmentinin "A" qovşağından aldığını təsdiqləməlidir. Amma aydın məsələdir ki, o bunu edə bilmir çünki, adətən məlumatın həcmi "FIN" seqmentinin "A" qovşağından ona göndərilmə zamanı məlum olmur. "A" qovşağından "B" qovşağına ötürülən informasiyanın bədəməl şəxs üçün heç bir maraq kəsb etmədiyindən o, sadəcə "A" seqmentinə "RST" bayraqlı paketi göndərir və bununla bağlantını kəsmiş olur.

3. *Xidmətdən imtina* (Denial of service - DoS). Bu tip hücumda bədəməl şəxs konkret servisi və ya kompüteri müvəqqəti iflic vəziyyətə gətirmək, şəbəkəni yenidən işə salmaq (reboot), qovşaqların yenidən iş qabiliyyətini bərpa etmək və ya yaddaşın doldurulmasını reallaşdırmağa çalışır. Bu halda bədəməl şəxs informasiyanı əldə etməyə deyil, o yalnız informasiyanı sahibi üçün əlçatmaz etməyə çalışır. DoS hücumlarının daha geniş yayılmış realizasiyalarına aşağıdakıları aid etmək olar:

• *DDoS* hücumlar – xidmətdən imtina tipli paylanmış hücumlar növüdür (DDoS - Distributed Denial of Service). Son illərin ən qəliz və yayılmış şəbəkə hücumlarındandır. DDoS-hücumlarının həyata keçməsi nəticəsində korporativ şəbəkənin qanuni istifadəçilərin, sistemin və resursların iş rejimi tam blokada vəziyyətinə salınır və şəbəkənin işi iflic vəziyyətə düşür. Bu tip hücumlardan sonra, adətən bərpa işləri həddindən çox vaxt tələb edir, bu isə öz növbəsində korporativ şəbəkənin işini uzun müddətə dayandırır. DDoS-hücumların əksəriyyətinin İnternet şəbəkəsinin təməl protokollarından olan TCP/IP protokolunun zəif nöqtələrindən sui-istifadə edərək, məsələn sistemlər tərəfindən SYN sorğularının emal prosesi zamanı reallaşdırılır. Bu vəziyyət bədəməl şəxsin öz anonimliyini qorumaq üçün yalançı ünvanlardan istifadə etməsi ilə daha da qəlizləşir.



Şəkil 3.1 Əks əlaqəsiz TCP - qoşulmanın imitasiyasından istifadə etməklə hücum sxemi

• *Ping of Death* hücum edilən qovşağa dataqram fraqmentlərinin göndərilməsindən ibarətdir. Bu dataqramların fraqmentləri yığıldıqdan sonra 65535 oktedi keçmiş olur. Xatırlatmaq yerinə düşərdi ki, IP-dataqramının "Fragment Offset" xanasının uzunluğu – 13 bitdir (yəni, maksimal ölçüsü 8192-yə bərabərdir) və fraqmentlərin sürüşməsi oktetlərin səkkizliyində ölçülür. Əgər dataqramın axırıncı fraqmenti bədəməl şəxs tərəfindən düzəldilibsə yəni sürüşmə "Fragment Offset"=8190 və uzunluq - 100-ə qədərdirsə, onda onun axırıncı oktetinin yığılan dataqramındakı yeri 8190*8+100=65620 (IP başlıqdan ən azı 20 oktet artıq) bu isə datqramın maksimal mümkün ola bilən qiymətindən daha artıqdır.

• *UDP flood.* Külli miqdarda "UDP" – məlumatlarla hücum edilən şəbəkəni dağıtmaqdan ibarətdir. Bədəməl şəxs külli miqdarda məlumatları idarə etmək üçün "UDP" servislərindən istifadə edərək, ixtiyari məlumata cavab olaraq göndərir. Misal olaraq: "echo" (port 7) və "chargen" (port 19) göstərmək olar. "A" (göndərənin portu –7) qovşağından "B" (göndərənin portu –19) qovşağına bədəməl şəxs məlumat göndərir. "B" qovşağı "A" qovşağının 7-ci portuna məlumat ilə cavab verir, bu isə öz növbəsində "B" qovşağının 19-cu portuna məlumatı geri göndərir və beləliklə bu proses sonsuza qədər davam edir (əslində isə bu proses məlumat şəbəkədə itənə qədər davam edir). Məşhur "UDP" trafiki "A" və "B" qovşaqlarının işlərini çətinləşdirir və bu yolla şəbəkədə tıxac əmələ gətirir.

• *SYN Flood* (*Neptune*) bədəməl şəxs tərəfindən hücum edilən qovşağın emal edə biləcəyindən dəfələrlə çox miqdarda TCP-nin SYN - seqmentlərinin göndərilməsindən ibarətdir. Hər bir SYN seqmentini alarkən TCP xüsusi "TCB" (Transmission Control Block) bloklar yaratmağa başlayır, yəni növbəti bağlantı üçün müəyyən resurslar ayırır və öz şəxsi SYN seqmentini göndərir. Amma o, bu sorğuya heç bir zaman cavab almayacaq. Bədəməl şəxs özünü əbəs yerə yormamaq üçün və heç bir iz

saxlamamaqdan ötrü o, öz SYN seqmentlərini mövcud olmayan bir və ya bir neçə göndərən qovşaq adından yollayacaq. Beləliklə TCP modulu bir neçə dəqiqədən sonra bu baş tutmayan bağlantını avtomatik olaraq kəsəcək. Bədəməl şəxs külli miqdarda SYN seqmentlərini generasiya etsə, onda o bağlantı yaratmaq üçün ayrılan bütün resursları zəbt etmiş olacaq və onun tərəfindən verilən sorğuları emal edib qurtarmayana qədər, TCP modulu yeni SYN seqmentlərini emal edə bilməyəcək. Müntəzəm olaraq bədəməl şəxs, yeni sorğular göndərməklə qovşağı müəyyən zaman kəsiyində blokada şəklində saxlaya bilər. Bu hücumun təsirinin bitirmək üçün bədəməl şəxs bir neçə "RST" bayraqlı seqmentlər göndərir ki, onlarda öz növbəsində yarımçıq bağlantıları kəsir və hücum edilən qovşağın resurslarını azad etmiş olur (şəkil 3.2).

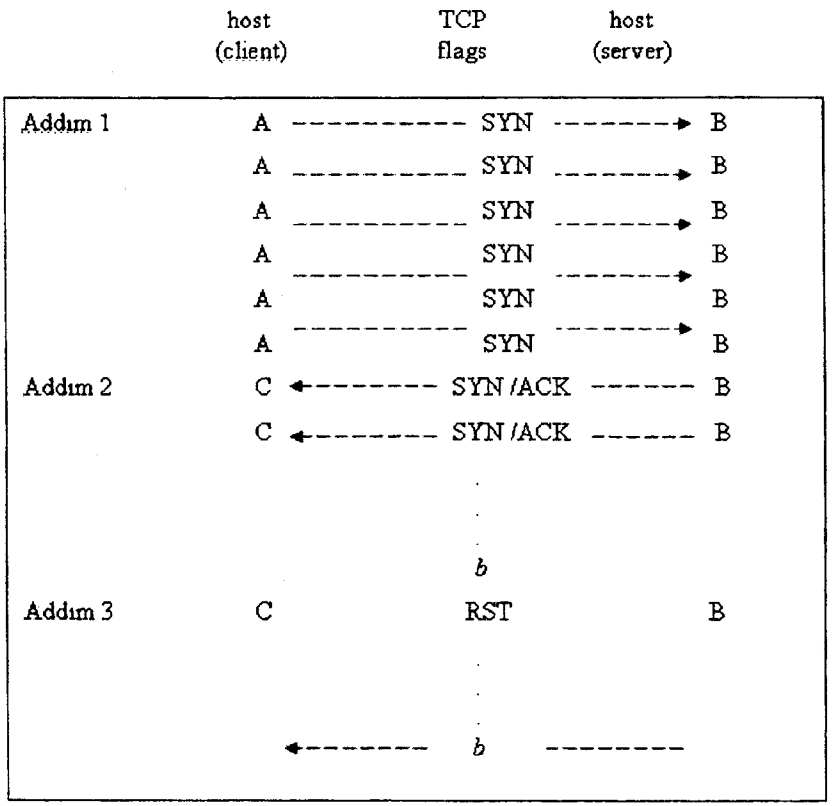
Hücumun əsas məqsədi qovşağı (serveri) elə vəziyyətə gətirməkdir ki, bu qovşaq qoşulmanı bərpa etmək üçün sorğuları qəbul edə bilməsin.

• *Land/Latierka* - bəzi əməliyyat sistemində TCP/IP stekinin reallaşmasında boşluqlardan istifadə etmək və əsas məramı kompüterin acıq portuna SYN bayrağı qeyd olunan yalançı TCP-paketləri göndərməkdən ibarətdir. Bu paketlərin ilkin ünvanı və portu müvafiq olaraq hücum edilən kompüterin ünvanı və portuna ekvivalentdir. Belə halda bu qovşaq özü-özünə qoşulmağa çalışan qovşağa çevrilir və sistem sonsuz dairə şəklində işləyir. Beləliklə sistem həddindən artıq yüklənməyə məruz qalır və bu da sistemin çökməsinə gətirib çıxarır.

• *WinNuke – Out of Band* ("növbəsiz", yəni yüksək prioritetlə) rejimində 139-cu port (NetBIOS Session/SMB) TCP – qoşulması üçün "URGENT" bayraqlı verilənlər göndərir.

Bu tip hücumun məqsədi şəbəkə vasitələri ilə əlaqələrin itirilməsidir.

• Arnudp100.c – IP ünvanın UDP-paketdə saxtalaşdırılmasıdır.



Şəkil 3.2 "TCP SYN flood" hücumun sxemi

• DoS – OSI etalon modelinin nəqliyyat və tətbiqi səviyyələrində reallaşan aktiv birtərəfli təsirə malik olan hücumdur.

4. *Şəbəkədə səhifələr üzərində uzaqdan idarəetmə.* Hücumun əsas məqsədi, hücum obyekti olan kompüterdə "şəbəkə casusu" işə salmaq vasitəsi ilə korporativ şəbəkənin hər hansı bir stansiyasının üzərində məsafədən idarə etmə hüququ əldə etməkdir. Bu günə bir neçə müxtəlif proqram məhsulları mövcuddur, onların funksiyası klaviaturadan daxil etməni izləyir və daxil olan simvolların siyahısını bir fayla yazır.

Belə proqramları adətən proqram qoşmaları adlandırırlar və onlar proqram vasitələrinin daxili strukturunda gizli şəkildə reallaşır. Məhz yerindən asılı olaraq onlar bədəməl şəxsə, müxtəlif yollarla sistemin dəyişdirilməsinə və sistemin məxfi resurslarına icazəsiz giriş hüququ imkanları yaradırlar. Adətən bədəməl şəxs tərəfindən ilk olaraq "*login*" proqramı dəyişdirilir. Məlum olduğu kimi, "*login*" proqramı sistemə daxil olmaq üçün istifadə olunur və bədəməl şəxs özünə elə parol və hüquq təyin edə bilər ki, o buna ixtiyari zaman sistemi tam idarə etmək imkanı verə bilər. Unix əməliyyat sistemində proqramlaşdırma kodunun əlçatan olması bu məsələni daha da asanlaşdırır. Bədəməl şəxs istədiyi sistem vasitəsinin proqram kodunu tapıb onu özünə sərf edən variantda dəyişdirə bilər. Təsadüfü deyil ki, indiki zamanda "*login*" proqramı ilə bərabər *in.telnetd, in.ftpd – demon, FTP və Telnet* giriş sessiyalarının xidmət olunması, host ilə mövcud olan bütün bağlantıları göstərən *netstat* proqramı, istifadəçilərin miqrasiyası və super-istifadəçi hüququnun əldə etməyə imkan verən "*su*" – proqramı da dəyişikliklərə məruz qalır.

Bundan başqa, bədəməl şəxslər tərəfindən bir sıra başqa hücum növləri mövcuddur. Bunlarda korporativ şəbəkələrin zəif yerlərinin və gizli imkanlarını skan əməliyyatı və hücum vasitəsi ilə yoxlanılmasıdır. Skan tipli hücumlara *ping sweeps, TCP* və *UDP* portların skan edilməsi, hücumunu misal göstərmək olar. Məsələn, *ping sweeps* hücumu nəticəsində aktiv kompüter şəbəkələri müəyyən olunur. TCP portlarının skan edilməsi isə kompüterin məxsus olduğu şəbəkənin daxili strukturunun və şəbəkə servislərinin işləmə prinsipini müəyyən etmək məqsədini güdür. TCP skan əməliyyatının bir neçə reallaşdırma metodu mövcuddur. Skan sessiyalarının adı, gizli (stealth) TCP bağlantıları yarımçıq əlaqəli və ya "Fin" seansları üçün istifadə olunur. Adətən bədəməl şəxs passiv skan əməliyyatından istifadə edir. Bunun istifadəsi zamanı TCP/IP SYN paketi bütün portlara ardıcıl və ya əvvəlcədən müəyyən olunmuş alqoritm şəklində

göndərilir. Xaricdən bağlantı alan TCP – portları üçün "SYN/ACK" paketləri geri dönəcək. Cavabları analiz etdikdən sonra, bədəməl şəxs tez bir zamanda hansı portda, hansı proqramın işlədiyini təyin edə bilər.

Bundan başqa bədəməl şəxslər, proqram təminatında gizli imkanlardan və ya proqramlaşdırma səhvlərindən istifadə edərək sistemə icazə verilməmiş giriş əldə edirlər. Bu tip hücumların ən geniş yayılanları aşağıdakılardır:

1. **CGI skriptlər** (proqramlar). Tipik boşluqlar adətən zərərli informasiyanın birbaşa sistemin əmrlər səthinə daxil olmasına səbəb olurlar. Gizli boşluqların istifadəsi isə sistemin daxili strukturu haqqında olan normal haldan, daha çox informasiyanı əldə etməyə imkan verir. CGI skriptin çox tanınmış səhvlərindən biri "phf" – kitabxanasıdır. Bu kitabxana adətən veb-serverdən ixtiyari faylın əldə olunması üçün istifadə olunur. Korporativ şəbəkələrdə aparılan uzun müşahidə nəticəsində müəyyən olan və bədəməl şəxs tərəfindən istifadə olunan biləcək digər CGI skriptlər isə bunlardır: TextCounter, GuesBook, Anyform, info2www, php.cgi və s.

2. **Veb-serverə hücumlar**. Bir çox serverlərin təhlükəsizlik sistemində boşluqlar olduğundan, bəzi fayların yerlərini fayl sistemində dəyişdirmək və ixtiyari faylı əldə etmək üçün, adların yerləşdiyi ünvanın sətrində müəyyən ardıcıllıqlar "../" mövcuddur. Çox yayılmış səhvlərdən biri – *sorğu* və ya *digər xanalardan birinin buferinin dolmasıdır.*

3. **Veb-brauzerə hücum**. Belə tip hücumlara URL - hücumları, HTTP - hücumları, HTML - hücumları, JavaScript - hücumları, ActiveX – hücumları və s. misal göstərmək olar. URL - xanalar HTTP başlıqda emal zamanı buferin dolmasına səbəb ola bilərlər. HTTP başlıqlar infromasiya qəbul etmək üçün nəzərdə tutulmayan xanalara informasiya ötürülməsi yolu ilə hücumu həyata keçirmək üçün istifadə oluna bilər.

JavaScript "faylın yüklənməsi" funksiyasının həyata keçməsinə kömək edir. Prinsip etibarı ilə bu proses təhlükəsizdir. Ona görə ki, istifadəçini "faylın adı" xanasını doldurduqdan sonra "submit" düyməsi vasitəsi ilə təsdiqləməyi tələb edir. Lakin, "JavaScript" bu prosesi avtomatlaşdıra bilər və bunun məntiqi nəticəsi olaraq, bədəməl şəxs veb səhifəni öz qovşağına köçürər. Beləliklə bu səhifəyə daxil olan istifadəçinin skriptdə əvvəlcədən göstərilmiş faylları bədəməl şəxsin qovşağına dərhal köçürülməsi prosesi başlanır.

ActiveX - hücumları ən təhlükəli hücumlar siyahısına aiddir. Çünki onlar etibarlı kod hesab olunurlar və həm lokal kompüterə, həm də əməliyyat sisteminin nüvəsinə tam giriş hüququna malikdirlər.

4. **Sendmail** - hücumları. *Sendmail* həddindən artıq çətin və geniş istifadə olunan proqramlardandır. Şəbəkədə tapılan təhlükəsizlik boşluqların xüsusi mənbəyi kimi qiymətləndirilir. Bədəməl şəxslər adətən buferin doldurulması metodunu tətbiq etməyə çalışırlar. Bundan başqa, "SMTP" – hücumları zamanı "VRFY" -ın tətbiq olunması da məsafədəki sistemin istifadəçilərinin adlarını müəyyən etmək üçün istifadə oluna bilər.

5. **IP-spoofing.** Müasir zamanda IP ünvanın dəyişdirilməsini (*spoof*) nəzərdə tutan bir sıra hücumlar mövcuddur. "IP-spoofing" adətən bir sıra başqa hücumların tərkib hissəsi kimi çıxış edir.

• ***Smurf.*** Bu hücum əsas məqsədi "ICMP Echo" – cavabları, hücum olunan qovşağa külli miqdarda lazımsız informasiyanın generasiyasından ibarətdir. Bədəməl şəxs külli miqdarda lazımsız informasiyanı yaratmaq üçün, bir neçə yalançı "Echo" - sorğuları hücum olunan qovşaq adından müxtəlif geniş yayımlanan şəbəkələrin ünvanlarına göndərir və onlarda gücləndirici rolunu oynamağa başlayır. "Echo" – sorğuları emal edən gücləndirici-şəbəkələrin həddindən böyük sayda olan qovşaqları, hücum olunan qovşağa cavabları göndərməyə başlayırlar. Bu hücumun

nəticəsində bədəməl şəxsin kompüteri, hücum edilən kompüter, bu kompüterin yerləşdiyi şəbəkə və həmçinin gücləndirici-şəbəkə özü də gələn cavab məlumatlarından müvəqqəti blokada şəraitinə düşür. Bundan başqa əgər hücum edilən şəbəkənin sahibi olan təşkilat İnternet xidmətlərini haqqını giriş və çıxış trafikinə görə provayderə ödəyirsə, onda bu çox böyük maddi ziyanla nəticələnə bilər.

• ***(TCP sequence number prediction)*** TCP – ardıcıllığı nömrəsinin əvvəlcədən ehtimal edilməsi – TCP bağlantı zamanı, paketlərin düzgün ardıcıllıqda bərpası üçün ardıcıllığın sıra nömrəsi seçilir,

• ***DNS poisoning*** – ardıcıllığının əvvəlcədən müəyyən edilməsi vasitəsi ilə DNS–serverləri domen adlarının rekursiv sorğularını istifadə edir. Beləliklə, istifadəçilərin sorğularına cavab verən DNS–server, özü də bilmədən DNS zəncirində növbəti bəndə çevrilir. Belə ardıcıllıqda istifadə olunan sıra nömrələrini asanlıqla tapmaq olar. Bədəməl şəxs DNS – serverə sorğunu göndərə bilər və onun cavabı elə quraşdırılır ki, o avtomatik olaraq zəncirdə olan növbəti serverin cavabına bənzəsin.

6. **Buffer overflow** (buferin dolması). Bu praktikada o zaman istifadə olunur ki, DNS–serverə uzun DNS adı (256 baytdan çox olsun), *statd overflow*, həddindən artıq uzun ad və s. göndərilsin.

Beləliklə, biz müasir korporativ şəbəkələrdə bəzi tip hücumlar və onların reallaşma texnologiyalarını nəzərdən keçirdik. Bu hücumlar korporativ şəbəkələrdə istifadə olunmuş təhlükəsizlik servislərinin pozulmasına yönəlmişdir. Təhlükəsizlik servislərinə yönəlmiş hücumları aşağıdakı qruplara bölmək olar (şəkil 3.3):

1. **Kəsilmə**

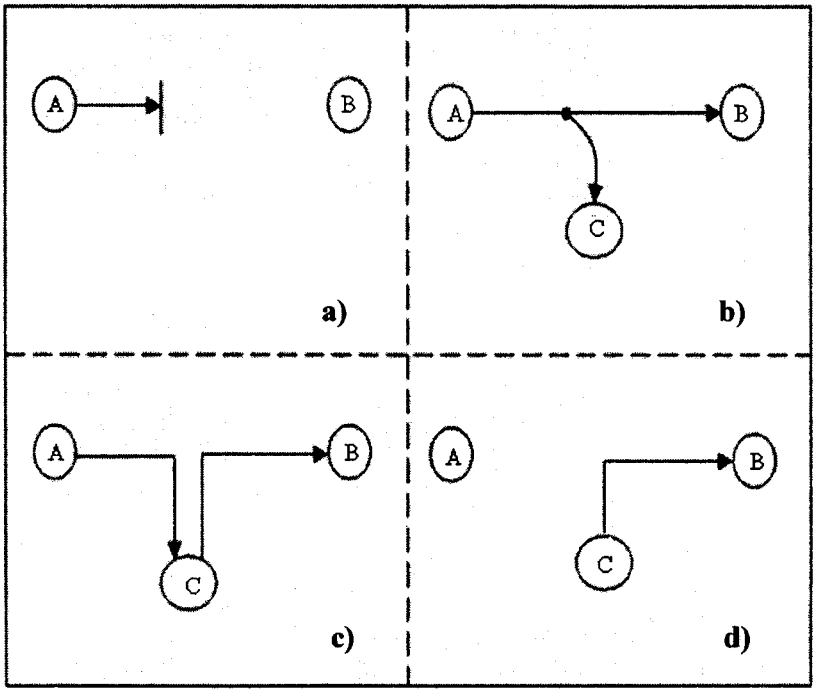
Bu halda sistem tam çökür və ya əl çatmaz olur. Bu tip hücumlar əlyetənliyin pozulmasına yönəlirlər.

2. **Ələ keçirmə**

Bu halda avtorizə edilməmiş istifadəçi məxfi informasiyanı əldə etmək hüququnu alır və onun surətini çıxarmaq imkanına malik olur. Adətən bu tip hücumlar həm tamlığın, həm də konfidensiallığın pozulmasına yönəlirlər.

3. **Dəyişdirilmə**

Bu tip hücum, mühafizə olunan (məsələm, məxfi informasiya) verilənlərə subyektin giriş imkanının əldə olunmasıdır. Halbuki həqiqətdə bədəməl şəxsin bu informasiyaya heç bir hüququ olmamalıdır. Bu zaman o nəinki informasiyanı əldə edir, həmçinin onu dəyişdirmək iqtidarındadır. Adətən bu tip hücumlar konfidensiallılıq və tamlığın pozulmasına yönəlirlər.



Şəkil 3.3 Təhlükəsizlik servislərinə olan hücumlar
a) *Kəsilmə;* **b)** *Ələ keçirmə;* **c)** *Dəyişdirilmə;* **d)** *Əvəz etmə (fabrikasiaya)*

4. **Əvəz etmə (fabrikasiaya - fabrication)**

Bu tip hücum zamanı sistemə icazəsiz yeni obyektlər (müxtəlif proqram modulları) daxil olunurlar. Bu hücumlar avtorizasiya və ya autentifikasiyanın pozulmasına yönəlirlər.

Müasir zamanda korporativ şəbəkələrdə informasiya təhlükəsizliyinin pozulmalarının qeydiyyatını aparan müxtəlif təşkilatlar mövcuddur. Bu siyahıya AusCERT, CERT/CC, JANET-CERT, RU-CERT və s. aid etmək olar. Bu təşkilatların hər biri ayrı-ayrılıqda müxtəlif kompüter şəbəkələrində baş verən insidentlərə reaksiya göstərir. Məsələn, RU-CERT təşkilatının məşğul olduğu əsas məsələlərdən biri RBNET şəbəkəsinə və İnternetin Rusiya hissəsinə aid olan istifadəçilərin kompüter şəbəkələrində baş verən insidentlərə reaksiya göstərmək və onları nizamlı şəkildə qeydə almaqdır. RU-CERT həm Rusiya, həm də bir sıra xarici İnsident Köm ək Komandalarına (IRT - Incident Response Team) yardım edir.

Həmçinin dayaq şəbəkənin istifadəçilərinə onların şəxsi resurslarına icazəsiz giriş problemlərinin həllində yardım göstərir və müvafiq göstərişlər verir. Bundan başqa, İnternetdə insidentlər baş verdikdən sonra, onların törəmə səbəblərinin araşdırılmasında və bir sıra mühafizə mexanizmlərində də yardımçı olur. Sadaladığımızdan savayı, RU-CERT təşkilatının funksiyasına: statistikanın yığılması və baş vermiş insidentlərin hesabatlarının generasiyası, CSIRT mərkəzləri ilə qarşılıqlı əlaqənin yaradılması və bilik almaqda kömək etmək, kompüter təhlükəsizliyinin baza anlayışları haqqında məsləhətlər, informasiya serverinə xidmət daxildir. Bu zaman əsas prioritetlərdən iri həcmli serverlərin resurslarına olan hücum tipləri bunlardır: RBNET regional altşəbəkəsinin qovşaqlarında reallaşan müxtəlif hücümların sayəsində şəbəkənin iş qabiliyyəti iflic vəziyyətə düşə bilər və informasiya resurslarının məhv edilməsinə səbəb ola bilər.

Yuxarıda sadalanan resurslara misal olaraq müxtəlif hücumları göstərmək olar. Serverlərdə administrativ hüquqları

almağa yönəlmiş, hostların məhv edilməsi və bu serverlərə zərərverici proqramların (sniffer proqramları, icazəsiz giriş əldə etməyə imkan verən proqramlar - *rootkit*, *back orifice*, parolu müəyyən etməyə imkan verən proqramlar və s.) yazılması ilə nəticələnən, virusların məqsəd yönlü şəkildə göndərilməsi, ayrı-ayrı istifadəçi hostlarına yönəlmiş DoS hücumlardır.

JANET-CERT təşkilatı da müxtəlif korporativ şəbəkələrdə ixtiyari informasiya təhlükəsizliyinin pozulması hallarını (insidentləri) qeydə alır. JANET-CERT təşkilatı xüsusi formadan istifadə edərək, yığılmış insidentləri bir qayda olaraq aşağıdakı siniflərə ayırır:

- avtorizə olunmamış giriş (*Unauthorized use*);
- parolun və identifikatorun ələ keçirilməsi (*Password capture*);
- müxtəlif hücum metodlarının istifadəsi (*Sniffer, Trojan horse*);
- xidmətdən imtina;
- snifferlər, müxtəlif viruslar (*Virus*);
- spamlar (*Spam*);
- SMTP, IMAP, DNS, SNMP ilə bağlı ixtiyari insidentlər CERT təşkilatının tövsiyəsinə əsasən hücumlar bir neçə tiplərə ayrılırlar (cədvəl 3.1).

Cədvəl 3.1

Hücumların tipləri və onların xarakteristikaları

Anonymous FTP abuse	Anonim girişə icazə verən FTP serverlərə yönələn hücum tipləri
Break-in	Sistemdə realizə olunan müxtəlif təhlükəsizlik servislərinin dayanmasına gətirib çıxaran hücumlar
Configuration error	İntensiv istifadə olunan proqramlarda istifadəçilərin düzgün konfiqurasiya olunmaması nəticəsində meydana çıxan boşluqlar

Cracked password	Asan tanına bilən parolların müəyyən olunmasına yönələn hücum tipi
DNS flooding	Bu hücum külli miqdarda DNS sorğuları ötürməklə adi istifadəçilərin İnternetdən istifadəsinə imkan vermir
Email bombardment	Əvvəlcədən seçilmiş bir elektron ünvana müxtəlif elektron ünvanlardan külli miqdarda məktubların göndərilməsi
Email spoofing	Başqa subyekt adından elektron məktubun göndərilməsi
Intruder gained root access	Bədəməl şəxs sistemə adi istifadəçi hüququnda daxil olub, sonra isə administrator hüququ almağa nail olur
Intruder installed Packed sniffer	Sistemdə xüsusi ələ keçirmə proqramı yerləşdirilir ki, o da öz növbəsində sistemi hücumlara açıq edir
Intruder installed Trojan horse program	Sistemə daxil olan bədəməl şəxs orada özünə məxsus olan "cəsus" proqramını yerləşdirir və onun köməkliyi ilə sistemə təkrar daxil olmaq asanlaşır
IP Hijacking	Bu hücum növü "IP-spoofing" və "gizli qulaqasma" hücumlarının kombinasiyasıdır
IP spoofing	IP-ünvanın dəyişdirilməsi vasitəsi ilə reallaşan hücum tipləri
Misuse of hostsre sources	"Hostsre" resurslarının düzgün istifadə olunmaması nəticəsində meydana gələn boşluqlar
NFS attack	Şəbəkə fayl strukturuna yönələn hücum tipi
NIS attack	Şəbəkəni idarə etməyə yönələn hücum tipi
Prank	Şəbəkə istifadəçilərinin profilinin düzgün yaradılmaması nəticəsində əmələ gələn zəif yerlərinə hücumlar

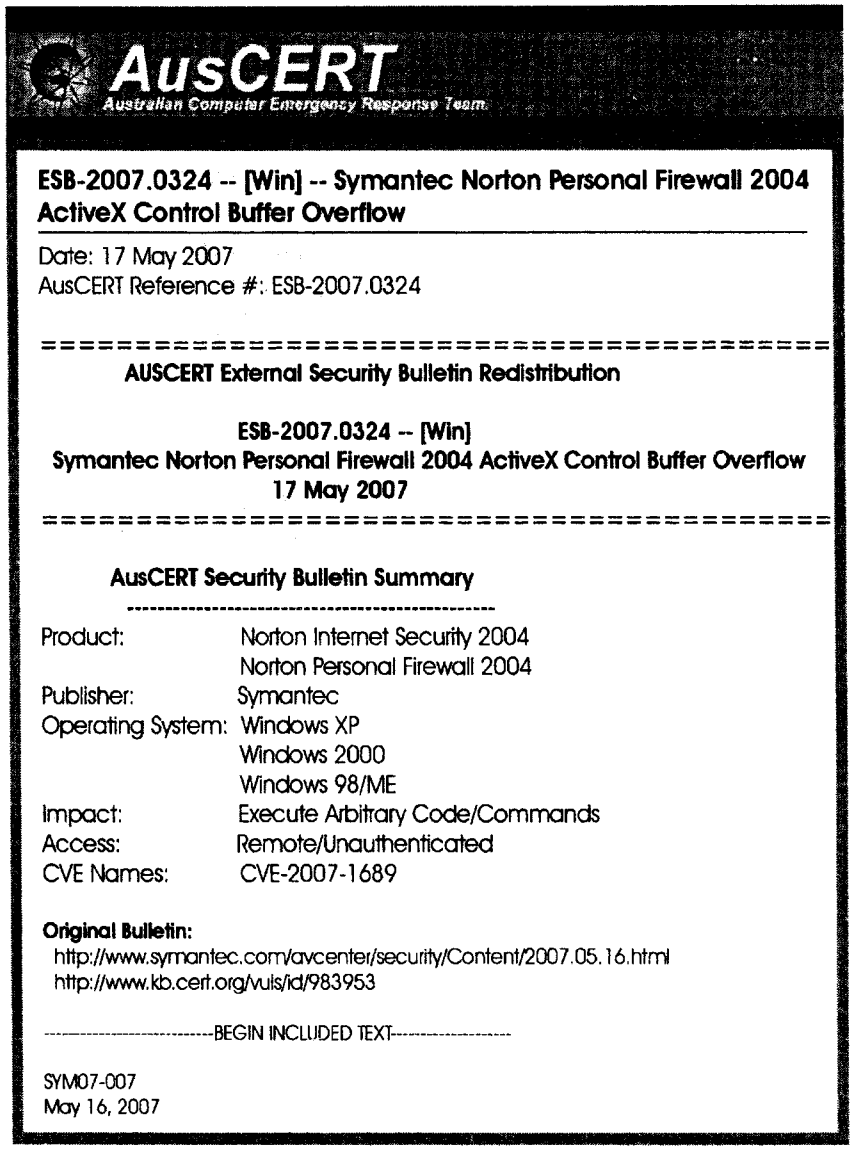
Probe, Scan, Scam	Acıq və istifadə olunan portların skan edilməsi və bu portlar vasitəsi ilə müxtəlif servislərə hücumun reallaşdırılması
Rlogin or rsh attack	Məsafədən giriş xidmətində olan boşluqlardan istifadəyə yönələn hücum tipi
Sendmail attack	SMTP portuna hücumlar
Telnet attack	Telnet protokolunda olan boşluqlardan istifadəyə yönələn hücum tipi
Worm, Virus	İstifadəçinin bilmədiyi sayda olan və sistemdə özü-üzünə idarə olunan, zərərli proqramların işləməsidir

AusCERT təşkilatında hər bir insident üçün ayrılıqda xarici təhlükəsizlik bülleteni (External Security Bulletin - ESB) buraxılır (şəkil 3.4). Bu bülletendə hücumun tipi, reallaşma texnologiyası, hücuma məruz qalan kompüterin əməliyyat sisteminin adı, versiyası və s. kimi zəruri məlumatlar yerləşdirilir (cədvəl 3.2). AusCERT təşkilatı kimi digər beynəlxalq təşkilatlar da mövcuddur ki, onlarda korporativ şəbəkələrdə baş verən insidentləri qeydə alırlar və baş vermiş insidentləri aradan qaldırmaqdan ötrü həlli yollarını təklif edirlər.

Cədvəl 3.2

İnformasiya təhlükəsizliyi pozulmalarının bəzi nümunələri

No	**Təhlükənin növü**	**Nəticəsi**	**Platforma**
1.	Denial of Service in the ptracet() system call	"Root" olmayan istifadəçilərə sistemi dağıtmağa imkan yaradır	AIX 3.2.x
2.	Buffer overfow in linnst	"Root" hüququnu əldə eləmək imkanı	Sun 5.3 əməliyyat sistemi



AusCERT
Australian Computer Emergency Response Team

ESB-2007.0324 -- [Win] -- Symantec Norton Personal Firewall 2004 ActiveX Control Buffer Overflow

Date: 17 May 2007
AusCERT Reference #: ESB-2007.0324

==========

AUSCERT External Security Bulletin Redistribution

ESB-2007.0324 -- [Win]
Symantec Norton Personal Firewall 2004 ActiveX Control Buffer Overflow
17 May 2007

==========

AusCERT Security Bulletin Summary

Product:	Norton Internet Security 2004
	Norton Personal Firewall 2004
Publisher:	Symantec
Operating System:	Windows XP
	Windows 2000
	Windows 98/ME
Impact:	Execute Arbitrary Code/Commands
Access:	Remote/Unauthenticated
CVE Names:	CVE-2007-1689

Original Bulletin:
http://www.symantec.com/avcenter/security/Content/2007.05.16.html
http://www.kb.cert.org/vuls/id/983953

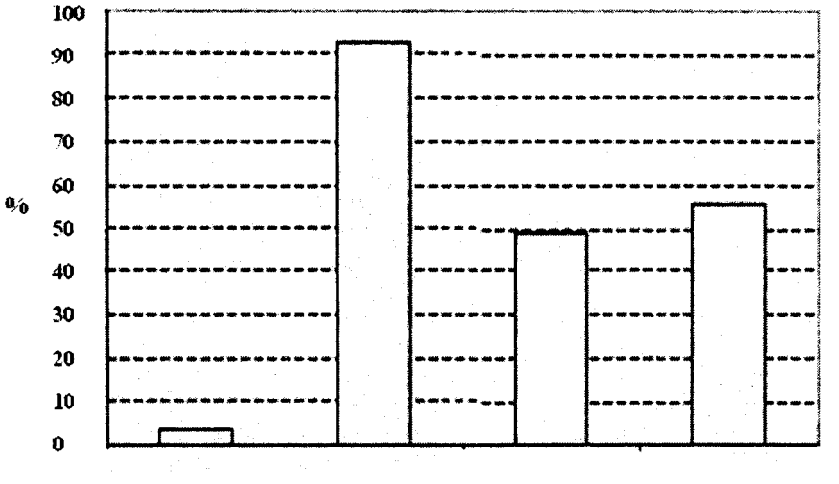
----------BEGIN INCLUDED TEXT----------

SYM07-007
May 16, 2007

Şəkil 3.4 Xarici təhlükəsizlik bülleteni (External Security Bulletin)

İndi isə statistik verilənlərin analizi əsasında, təhlükələri təhlükəsizlik servisləri qruplarına ayıraq. Statistik verilənlər kimi CERT təşkilatlarında qeydiyyatdan keçmiş insidentlərin bülletenlərindən istifadə edəcəyik. Bu kitabda əsasən Janet CERT insidentləri qeydə alan beynəlxalq təşkilatın xarici bülletenlərinə baxılmışdır. Araşdırmalar təqribən 3 il müddəti əhatə edir və bu müddət ərzində dayanmadan hər bir günün statistikası (yəni korporativ şəbəkələrdə baş verən və qeydiyyata düşən bütün insidentlərin siyahısı və izahı) müfəssəl şəkildə analiz olunmuşdur. Aparılan analizlər nəticəsində təhlükəsizlik pozulmalarını təhlükəsizlik servislərinə görə qruplara ayırmaq mümkündür. Qruplaşdırmanın nəticəsi şəkil 3.5-də göstərilmişdir.

Bu verilənlər korporativ şəbəkənin layihələndirilməsi mərhələsində təhlükəsizliyin qiymətləndirilməsində istifadə oluna bilər.



1 - konfidensiallıq; 2 - avtorizasiya; 3 - tamlıq; 4 - əlyetənlik

Şəkil 3.5 Hücumların təhlükəsizlik servisləri üzrə paylanması histoqramı

3.2. Korporativ şəbəkənin informasiya təhlükəsizliyinin qiymətləndirilməsi üçün uyğun etibarlılıq modelinin seçilməsi

Məlum olduğu kimi informasiya texnologiyalarının belə geniş yayıldığı zamanda korporativ şəbəkələrdə informasiya təhlükəsizliyinin pozulmaları haqqında bəs qədər statistik verilənlər mövcuddur. Bu statistik verilənlər müxtəlif çağırış (və ya çağırışa cavab) mərkəzləri, yəni CERT təşkilatları tərəfindən məsələn, AusCERT, JANET CERT, RU-CERT və s. qeydə alınmışdır.

Korporativ şəbəkələrdə informasiya təhlükəsizliyi pozulmalarının statistik verilənlərini bu sistemlərin mühafizəlilik dərəcəsinə sınağın nəticəsi kimi də qiymətləndirmək olar. Bu halda uyğun gələn proqram təminatının etibarlılığı modelini seçməklə, korporativ şəbəkələrdə informasiya təhlükəsizliyinin qiymətləndirilməsinin metrikasını işləmək olar.

Bu günə, müxtəlif olan proqram təminatının etibarlılığı modelləri mövcuddur. Bu modellərin hər biri hər hansı bir ehtimal üzərində qurulub. Ona görə də, bu və ya digər modeli seçməmişdən öncə, korporativ şəbəkələrdə informasiya təhlükəsizliyinin pozulmalarının statistik verilənlərə xas olan bir sıra xassələri nəzərdən keçirək.

CERT təşkilatlarda olan informasiya təhlükəsizliyinin pozulmaları haqqında statistik verilənlər müxtəlif kompüter şəbəkələrinin istifadəsi zamanı toplanmışdır. Bu verilənlər, xüsusi verilənlər bazasında ayrı-ayrı pozulmalar şəklində müəyyən zaman intervalı ilə (ay, kvartal, il) yerləşdirilib. Onları müxtəlif sistemlərin mühafizəlilik dərəcəsinin yoxlanılması kimidə başa düşmək olar. Bu halda ayrı-ayrı informasiya təhlükəsizliyinin pozulmaları, sınaq zamanı proqram təminatının sapmalarına (və ya proqram təminatında səhvlərin tapılması) və ayrı-ayrı zaman kəsikləri isə sınaq müddətinə bərabər tutulur.

CERT təşkilatında olan korporativ şəbəkələrin informasiya təhlükəsizliyinin pozulmaları haqqında statistik verilənlərini $\langle U, T, \eta(T) \rangle$ üçlük kimi vermək olar, harada ki, $U = \{u_f\}$, $f = \overline{1, N}$ - şəbəkədə informasiya təhlükəsizliyinin pozulmaları növlərinin çoxluğudur; $T = \{t_i\}$, $i = \overline{1, n}$ - kəsişməyən zaman intervallarının çoxluğudur; $\eta(T) = \eta_f \{t_i\}$, $i = \overline{1, n}$, $f = \overline{1, N}$ - təsadüfü kəmiyyətlər çoxluğudur, yəni t_i zaman intervalında f tipli informasiya təhlükəsizliyinin pozulmalarının sayı.

İnformasiya təhlükəsizliyinin pozulmaları haqqında statistik verilənlər müxtəlif korporativ şəbəkələrə məxsus olduğundan, ixtiyari kəsişməyən $t_1, t_2, ..., t_n$ zaman intervallı dəsti üçün bu zaman intervalında olan hər növ pozulmanın sayı $\eta_f(t_1), \eta_f(t_2), ..., \eta_f(t_n)$ qarşılıqlı asılı olmayan təsadüfü kəmiyyətlər şəklində ifadə olunur. Bu faktı nəzərə alaraq informasiya təhlükəsizliyi axınını izsiz axın kimi qəbul etmək olar.

Δt zaman kəsiyində eyni vaxtda iki və ya daha çox informasiya təhlükəsizliyinin pozulmaları ehtimalı sıfıra bərabər olmasını qəbul edək, yəni:

$$\lim_{\Delta t \to 0} \frac{q(2, \Delta t)}{\Delta t} = 0 ,$$

burada $q(2, \Delta t)$ - eyni vaxtda ən azı iki pozulmanın Δt zaman kəsiyində baş vermə ehtimalıdır. Bu fərziyyə tam şəkildə yol verilməndir. Bu halda informasiya təhlükəsizliyinin pozulmaları axınını ordinar axın sinfinə aid etmək olar.

Korporativ şəbəkələrdə informasiya təhlükəsizliyinin pozulmaları axının digər vacib xassəsi qeyri-stasionarlıqdır. Qeyri-stasionarlığın əsas səbəbi qəsdən törədilən hücumlar və ya

viruslardır. Məsələn, 2003-cü ildə «Slammer» virusu üç dəqiqə hücum ərzində dünya üzrə 75000 serveri iflic vəziyyətə salmışdır. Əlbəttə ki, belə hadisələr informasiya təhlükəsizliyinin pozulmalarını qısa zaman intervalında kəskin artmasına səbəb olur. Bu da öz növbəsində informasiya təhlükəsizliyinin pozulmaları axının qeyri-stasionarlıq xassəsinə gətirib çıxarır.

Yuxarıda qeyd olunanları nəzərə alsaq, korporativ şəbəkələrdə informasiya təhlükəsizliyinin pozulmaları axını, qeyri-stasionar (qeyri-həmcins) Puasson axını kimi xarakterizə oluna bilər. Beləliklə bu üç xassəni özündə cəmləyən axına qeyri-həmcins Puasson axını deyilir. Ona görə də, lazımi etibarlılıq modelini qeyri-həmcins Puasson prosesi (QHPP) əsasında qurulan modellər siyahısından seçmək lazımdır.

Müxtəlif QHPP modellərini müqayisə etmək üçün kvadratik xətalar cəmindən meyar kimi istifadə edirik, yəni

$$\sigma = \sum_{i=1}^{n} \left[y_i - \hat{m}(t_i) \right]^2 , \qquad (3.1)$$

burada y_i- t_i zamanı ərzində olan imtinaların ümumi cəmidir; $\hat{m}(t_i)$- t_i zamanı ərazində imtinaların yığılmış sayının qiymətidir.

Belə halda σ parametrinin qiyməti nə qədər kiçik olarsa, o qədər də model uğurlu sayılacaq. İlkin verilənlər kimi yoxlanış sisteminin monitorinq edən proqramın sınağı nəticəsində əldə olunan real verilənlərdən istifadə edək. Bu verilənlər cədvəl 3.4 – də göstərilmişdir. Goel-Okomuto, Delayed S-shaped, Yamada exponential, Yamada Rayleigh, Yamada imperfect debugging model, Pham Nordman и Pham Zhang kimi məşhur proqram təminatının etibarlılıq modelları nəzərdən keçirilmişdir.

σ parametrini təyin etmək üçün (3.1) düsturuna əsasən aparılan hesabatlar göstərdi ki, Pham-Zhang (σ=59,5) etibarlılıq modeli, ən uyğun olanıdır.

Korporativ şəbəkələrdə informasiya təhlükəsizliyinin pozulmaları təhlükələri ildən-ilə durmadan yeniləri ilə əvəz olunduğundan, etibarlılıq modelini seçərkən bu amilə diqqət yetirmək vacib məsələlərdən biridir. Ona görə də, QHPP modelini seçdikdə bu faktora ciddi yanaşmaq lazımdır. Məhz, bu səbəbdən "NHPP imperfect debugging model Pham" modeli korporativ şəbəkələrdə informasiya təhlükəsizliyinin qiymətləndirilməsi üçün ən uyğun gələn etibarlılıq modelidir.

Sözü gedən modeldə yeni yaranan təhlükələri nəzərə almaq imkanı vardır. Bu modelin modifikasiya olunmuş variantından istifadə edəcəyik.

"NHPP imperfect debugging model Pham" modelində $m(t)$ funksiyası aşağıda göstərilən diferensial tənliklərlə təyin olunur:

$$\frac{\partial}{\partial t}[m(t)] = b[n(t) - m(t)]$$

Cədvəl 3.3

Etibarlılıq modelləri

Etibarlılıq modelinin adı	**Etibarlılıq modelinin tipi**	**m(t) funksiyası**
Goel–Okumoto * (G–O)	Çökük (Concave)	$m(t) = a(1 - e^{-bt})$ $a(t) = a$ $b(t) = b$
Delayed S-shaped	S-şəkilli (S-shaped)	$m(t) = a(1 - (1 + bt)e^{-bt})$ $a(t) = a$ $b(t) = \frac{b^2 t}{1 + bt}$

Etibarlılıq modelinin adı	**Etibarlılıq modelinin tipi**	**m(t) funksiyası**
Inflection S-shaped	Çöküк	$m(t) = \frac{a(1-e^{-bt})}{1+\beta e^{-bt}}$ $a(t) = a$ $b(t) = \frac{b}{1+\beta e^{-bt}}$
Yamada exponential	Çöküк	$m(t) = a(1-e^{-r\alpha(1-e^{(-\beta t)})})$ $a(t) = a$ $b(t) = r\alpha\beta e^{-\beta t}$
Yamada Rayleigh	S-şəkilli	$m(t) = a(1-e^{-r\alpha(1-e^{(-\beta t^2/2)})})$ $a(t) = a$ $b(t) = r\alpha\beta e^{-\beta t^2/2}$
Yamada imperfect debugging model (1)	S-şəkilli	$m(t) = \frac{ab}{a+b}(e^{\alpha t} - e^{-bt})$ $a(t) = ae^{\alpha t}$ $b(t) = b$

Etibarlılıq modelinin adı	**Etibarlılıq modelinin tipi**	**m(t) funksiyası**
Yamada imperfect debugging model (2)	S-şəkilli	$m(t) = a[1 - e^{-bt}][1 - \frac{\alpha}{b}] + \alpha at$ $a(t) = a(1 + \alpha t)$ $b(t) = b$
Pham–Nordmann	S-şəkilli və çökük	$m(t) = \frac{a[1 - e^{-bt}][1 - \frac{\alpha}{b}] + \alpha at}{1 + \beta e^{-bt}}$ $a(t) = ae^{\alpha t}$ $b(t) = b$
Pham–Zhang	S-şəkilli və çökük	$m(t) = \frac{1}{(1 + \beta e^{-bt})}[(c + a) \times$ $\times (1 - e^{-bt}) - \frac{a}{b - \alpha} \times$ $\times (e^{-\alpha t} - e^{-bt})]$ $a(t) = c + a(1 - e^{-\alpha t})$ $b(t) = \frac{b}{1 + \beta e^{-bt}}$

***Qeyd:** *Cədvəldə modellərin adları orijinal formada (İngilis versiyasında) göstərilib.*

$$\frac{\partial}{\partial t}[n(t)] = \beta \frac{\partial}{\partial t}[m(t)]$$

$$n(0) = a$$

$$m(0) = 0$$

burada, a - tapılan proqram səhvlərinin orta qiyməti;

b - tapılan proqram səhvlərinin intensivliyi;

$m(t)$ - t zamanı ərzində tapılan proqram səhvlərinin orta qiyməti;

$n(t)$ - tapılan proqram səhvlərinin orta qiyməti ilə t zamanı ərzində tapılan səhvlərinin qiymətinin cəmi;

β - yeni təhlükələri nəzərə almaq imkanını verən, əmsal.

β $(0 \le \beta < 1)$ əmsalı əvvəlcədən müəyyən olunur. Yuxarıda göstərilən diferensial tənliklər sistemini həll edərək növbəti ifadələri əldə etmiş olarıq:

Cədvəl 3.4

Proqram təminatının sapmaları

Gün	Sapmaların sayı	Gün	Sapmaların sayı	Gün	Sapmaların sayı	Gün	Sapmaların sayı	Gün	Sapmaların sayı
1	5	23	4	45	10	67	0	89	0
2	5	24	4	46	3	68	1	90	0
3	5	25	2	47	3	69	1	91	0
4	5	26	4	48	8	70	0	92	0
5	6	27	3	49	5	71	0	93	0
6	8	28	9	50	1	72	0	94	0

7	2	29	2	51	2	73	1	95	0
8	7	30	5	52	2	74	0	96	1
9	4	31	4	53	2	75	0	97	0
10	2	32	1	54	7	76	0	98	0
11	31	33	4	55	2	77	1	99	0
12	4	34	3	56	0	78	2	100	1
13	24	35	6	57	2	79	0	101	0
14	49	36	13	58	3	80	1	102	0
15	14	37	19	59	2	81	0	103	1
16	12	38	15	60	7	82	0	104	0
17	8	39	7	61	3	83	0	105	0
18	9	40	15	62	0	84	0	106	1
19	4	41	21	63	1	85	0	107	0
20	7	42	8	64	0	86	0	108	0
21	6	43	6	65	1	87	2	109	1
22	9	44	20	66	0	88	0	110	0

$$m(t) = \frac{a}{(1-\beta)}\left[1 - e^{-(1-\beta)bt}\right]$$

$$\lambda(t) = abe^{-(1-\beta)bt},$$

burada $\lambda(t)$ - pozulmaların əmələgəlmə intensivliyidir.

$$n(t) = \frac{a}{(1-\beta)}\left[1 - \beta e^{-(1-\beta)bt}\right]$$

Bu halda $[t, t+z]$ zaman intervalında informasiya təhlükəsizliyinin pozulması baş verməyəcəyi ehtimalı aşağıdakı düsturla təyin oluna bilər:

$$P(z/t)=e^{-\left[\frac{a}{1-\beta}\left(e^{-(1-\beta)bt}\right)\left[1-e^{-(1-\beta)bz}\right]\right]}, \qquad (3.2)$$

a və b parametrlərini təyin etmək üçün maksimal mümkünlük üsulundan istifadə edirik. Riyazi statistikanın bir sıra məsələləri ona gətirir ki, paylanma zamanı bəzi, əvvəlcədən məlum olmayan parametrləri qiymətləndirmək mümkün olsun.

Maksimal mümkünlük üsuluna əsasən axtarılan parametrin qiyməti yerinə, keçirilən sınaqların nəticəsində ən çox ehtimal oluna bilən kəmiyyət qəbul olunur. Qəbul edək ki, verilənlər (t_i, y_i) şəklində təsvir olunub, burada y_i- t_i zamanına qədər, tapılan hər bir təhlükəsizlik servisi üçün pozulmalar sayının yığılmış cəmidir. Proqram təminatında səhvlərin tapılması prosesinin qeyri-həmcins Puasson prosesi ilə xarakterizə olunmasını nəzərə alaraq, (t_i, y_i), $i=1,2,...,n$ məlum verilənlər üçün, $L(a,b)$ mümkünlük funksiyası aşağıdakı kimi təyin olunur:

$$L(a,b)=\prod_{i=1}^{n}\frac{\left[m(t_i)-m(t_{i-1})\right]^{(y_i-y_{i-1})}}{(y_i-y_{i-1})!}e^{-[m(t_i)-m(t_{i-1})]} \qquad (3.3)$$

burada

$$m(t_i)=\frac{a}{(1-\beta)}\left[1-e^{-(1-\beta)bt_i}\right].$$

(3.3) mümkünlük funksiyasını loqarifmləyərək aşağıdakı ifadəni alırıq:

$$\ln[L(a,b)]=\sum_{i=1}^{n}\left[\begin{array}{l}(y_i-y_{i-1})\ln[m(t_i)-m(t_{i-1})]- \\ -\ln[(y_i-y_{i-1})!]-[m(t_i)-m(t_{i-1})]\end{array}\right]$$

Sonra loqarifmdən mümkünlük funksiyasının a və b məchul parametrlərinə görə xüsusi tərtib törəmə alaraq, növbəti sistem tənliyini əldə etmiş olarıq

$$\begin{cases} a = \dfrac{y_n}{\dfrac{1}{1-\beta}\left[1 - e^{-(1-\beta)bt_n}\right]} \\ \sum_{i=1}^{n}(y_i - y_{i-1})\dfrac{(1-\beta)[t_i e^{-(1-\beta)bt_i} - t_{i-1}e^{-(1-\beta)bt_{i-1}}]}{e^{-(1-\beta)bt_{i-1}} - e^{-(1-\beta)bt_i}} = \\ = at_n e^{-(1-\beta)bt_n} \end{cases} \tag{3.4}$$

(3.4) sistem tənliyini həll edərək a və b parametrlərinin qiymətlərini asanlıqla tapmaq olar. Tapdığımız a və b parametrlərinin qiymətlərini (3.2) düsturuna qoyaraq $P(z/t)$ qiymətini təyin edirik.

3.3. Layihələndirilmə mərhələsində korporativ şəbəkənin informasiya təhlükəsizliyinin qiymətləndirilməsi metodu

Korporativ şəbəkələrin geniş inkişaf etməsi, onların ümumi istifadə üçün nəzərdə tutulan müxtəlif informasiya sistemləri ilə inteqrasiyası, nəzərə çarpacaq üstünlükləri ilə bərabər, bir sıra yeni informasiya təhlükəsizliyi ilə bağlı problemlər törədir. Bu problemlərin yaranma səbəbi ilk olaraq, korporativ şəbəkələrdə istifadə olunan proqram-aparat təminatının müxtəlif və mürəkkəb olması ilə, şəbəkənin informasiya mübadiləsində iştirak edən həddindən çox sayda qovşaqlar olması, coğrafi baxımdan paylanmış ərazidə yerləşməsi, şəbəkənin bütün seqmentlərini nəzarət altında saxlamaq mümkün olmaması və korporativ şəbəkənin xaricdən olan istifadəçilərə (müştərilərə, tərəfdaşlara və

s.) açıq olması ilə xarakterizə olunur. Heçdə təsadüfü deyil ki, son illər korporativ şəbəkənin layihələndirilməsi onun təhlükəsizlik sisteminin yaradılması ilə bərabər aparılır.

Məlum olduğu kimi, korporativ şəbəkənin informasiya təhlükəsizliyini təmin etmək üçün təhlükəsizlik servisləri yığımı işlənir ki, onlarında daxilində informasiya təhlükəsizliyini təmin edən funksiyalar realizə olunur. Hal-hazırda korporativ şəbəkələr üçün vahid bir informasiya təhlükəsizliyini təmin edən unikal bir struktur və ya mexanizm yoxdur. Hər bir şirkət öz fəaliyyəti və ya şəbəkəsi ilə bağlı özünə məxsus və digərlərindən fərqlənən tələblər paketinə, problemlərə və prioritetlərə malikdir. Ona görə də korporativ şəbəkə layihələndirilən zaman, təhlükəsizlik siyasətindən asılı olaraq, müxtəlif təhlükəsizlik servisləri yığımı realizə olunur. Bu halda korporativ şəbəkənin informasiya təhlükəsizliyini korporativ şəbəkədə realizə olunan təhlükəsizlik servislərindən asılı olaraq qiymətləndirilməsi həddindən artıq vacib məsələdir.

Digər tərəfdən, proqram təminatının etibarlılığı, müəyyən edilmiş zaman intervalında və əvvəlcədən təyin edilmiş şəraitdə proqramın sapmadan işləməsi ehtimalıdır. Bu halda proqram təminatının sapması (iş qabiliyyətinin pozulması) dedikdə, proqram təminatının əvvəlcədən təyin olunmuş qaydalardan ixtiyari şəkildə kənara çıxması başa düşülür. Analoji olaraq, korporativ şəbəkənin informasiya təhlükəsizliyinin pozulması dedikdə, ixtiyari hadisə nəticəsində korporativ şəbəkəyə dəyən ziyan, verilənlərin dəyişdirilməsi və ya ələ keçirilməsi, xidmətdən imtina kimi hallar və s. başa düşülə bilər. Yəni, korporativ şəbəkənin informasiya təhlükəsizliyinin pozulması verilmiş sistemin tələblərindən ixtiyarı yayınmadır. Bu baxımdan korporativ şəbəkənin informasiya təhlükəsizliyi, etibarlılıq nəzəriyyəsi terminləri çərçivəsində izah oluna bilər.

Fərz edək ki, $S = \{s_j\}, j = \overline{1,k}$ təhlükəsizlik servislərinin çoxluğudur və layihələndiriləcək korporativ şəbəkədə istifadə oluna bilər. Korporativ şəbəkə, onda realizə olunan təhlükəsizlik servislərinin miqdarı və tərkibindən asılı olaraq, müxtəlif mühafizəlilik dərəcəsi əldə edə bilər. Təbiidir ki, korporativ şəbəkə layihələndirilən zaman, ayrı-ayrı təhlükəsizlik servislərinin korporativ şəbəkənin informasiya təhlükəsizliyinə necə təsir göstərəcəyi məlum olmur.

Ona görə də bunlar arasında olan əlaqəni ümumi halda çoxdəyişənli xətti reqressiya tənliyi şəklində vermək olar.

$$M_S = \alpha_0 + \sum_{j=1}^{k} \alpha_j x_j , \qquad (3.5)$$

burada,

$\alpha_0, \alpha_1, ..., \alpha_k$ çoxdəyişənli xətti reqressiya əmsalları;

$x_1, x_2, ..., x_k$ - təhlükəsizlik servislərini xarakterizə edən parametrlər ;

M_S - korporativ şəbəkənin informasiya təhlükəsizliyinin qiymətləndirilmə metrikası.

(3.5) düsturunda x_j, $j = \overline{1,k}$ yerinə etibarlılıq xarakteristikası istifadə etmək təklif olunduğundan, M_S ehtimal edilən bir dəyişən olacaq.

(3.5) düsturunun konkret formasını təyin etmək üçün, $(M_S, x_1, x_2, ..., x_k)$ tipli verilənlər çoxluğunu əldə etmək zəruridir.

Yuxarıda qeyd olunduğu kimi, layihələndirilən zaman korporativ şəbəkədə təhlükəsizlik siyasətindən asılı olaraq, müxtəlif təhlükəsizlik servisləri ixtiyari kombinasiyada realizə

oluna bilərlər. Bu kombinasiyaların sayı $L=2^k$. $x_1, x_2, ..., x_k$ verilənlər çoxluğunu formalaşdırmaq məqsədi ilə təhlükəsizlik servislərinin hər bir realizə olunma variantı üçün aşağıdakı proseduradan istifadə olunur:

$$x_j^{(l)} = \begin{cases} P_j(z/t), & \textit{əgər } l \textit{ variantında } j \textit{ servisi realizə olunub} \\ 0, & \textit{əks halda} \end{cases}$$

$$l = \overline{1,L}$$

Beləliklə $x_1, x_2, ..., x_k$ verilənlər çoxluğunu əldə etmiş oluruq.

M_S üçün verilənlər çoxluğunu formalaşdırmaq məqsədi ilə təhlükəsizlik servislərinin pozulmaları haqqında statistik verilənləri istifadə edərək, ilkin olaraq $t_1, t_2, ..., t_n$ zaman intervalında hər bir təhlükəsizlik servisi üçün pozulmaların yığılmış cəminin qiymətini təyin edirik (cədvəl 3.5).

Onda layihələndirilən korporativ şəbəkədə təhlükəsizlik servisinin l realizə olunma variantında növbəti ifadəni almış oluruq

$$M_S^{(l)} = 1 - \frac{\sum_{g \in A_l} y_{n,g}}{\sum_{j=1}^{k} y_{n,j}}, \quad g \in J, l = \overline{1,L}, \qquad (3.6)$$

burada,

A_l - l variantında korporativ şəbəkədə realizə olunmayan təhlükəsizlik servislər çoxluğudur; J - təhlükəsizlik servislərinin indekslər çoxluğudur.

(3.6) düsturuna əsasən,

- əgər layihələndiriləcək korporativ şəbəkədə bütün növ təhlükəsizlik servisləri istifadə olunubsa, onda $M_s = 1$ olar;
- əgər layihələndiriləcək korporativ şəbəkədə heç bir təhlükəsizlik servisi istifadə olunmayıbsa, onda $M_s = 0$ olar.

Cədvəl 3.5

Təhlükəsizlik pozulmalarının yığılmış cəmlər sayının hesablanma ardıcıllığı

Vaxt	***j* saylı təhlükəsizlik servisinin pozulmaları**	***j* saylı təhlükəsizlik servisinin pozulmalarının yığılmış cəmlər sayının**
t_1	$\nu_j(t_1)$	$y_{1,j} = \nu_j(t_1)$
t_2	$\nu_j(t_2)$	$y_{2,j} = \nu_j(t_1) + \nu_j(t_2)$
⋮	⋮	⋮
t_i	$\nu_j(t_i)$	$y_{i,j} = \nu_j(t_1) + \nu_j(t_2) + ... + \nu_j(t_i)$
⋮	⋮	⋮
t_n	$\nu_j(t_n)$	$y_{n,j} = \nu_j(t_1) + \nu_j(t_2) + ... + \nu_j(t_i) + ... + \nu_j(t_n)$

Beləliklə, $(M_S, x_1, x_2, ..., x_k)$ tipli verilənlər çoxluğunu əldə etmiş oluruq və bu da, (3.5) düsturunda olan xətti reqressiyanın əmsallarını təyin etməyə imkan verir. Nəhayət

korporativ şəbəkədə layihələndirilmə mərhələsində informasiya təhlükəsizliyini qiymətləndirmək üçün konkret ifadə almış oluruq.

Bu metrikanı istifadə edərək, mühafizəli korporativ şəbəkə üçün müxtəlif aspektlərdə fərqli məsələlər həll etmək, daha dəqiq desək "təhlükəsizlik-qiymət" anlayışını daxil etsək, onda layihələndiriləcək korporativ şəbəkədə təhlükəsizlik servislərinin optimal heyətinin və miqdarının seçilməsi məsələsini qarşıya qoyub həll etmək mümkündür.

Bundan başqa bu metrikanı istifadə edərək, $P_s = 1 - M_s$ düsturu vasitəsi ilə layihələndiriləcək korporativ şəbəkədə təhlükəsizliyin pozulmasını qiymətləndirmək mümkündür ki, bu da öz növbəsində layihələndirilmə mərhələsində riski qiymətləndirmək imkanı verir.

JANET/CC təşkilatında 3 il ərzində toplanan informasiya təhlükəsizliyi pozulmalarının statistik verilənləri nəzərdən keçirək. Bu verilənlər dörd təhlükəsizlik servisi üzrə siniflərə bölünüblər – konfidensiallıq, tamlıq, əlyetənlik və avtorizasiya (cədvəl 3.6). 3.6 cədvəlindən göründüyü kimi, baxılan müddətdə cəmi 1119 informasiya təhlükəsizliyi pozulması hadisəsi baş vermişdir.

3.7 cədvəlinin verilənlərinə əsasən və (3.4) düsturundan istifadə edərək, hər bir təhlükəsizlik servisi üçün məchul a və b parametrlərini təyin edirik:

konfidensialliq üçün $\hat{a}_1 = 30.7407,\ \hat{b}_1 = 0.3408$

tamlıq üçün $\hat{a}_2 = 397.645,\ \hat{b}_2 = 0.3336$

əlyetənlik üçün $\hat{a}_3 = 352.2571,\ \hat{b}_3 = 0.5331$

avtorizasiya üçün $\hat{a}_4 = 584.4723,\ \hat{b}_4 = 0.5678$

Korporativ şəbəkənin hər bir təhlükəsizlik servisi üçün pozulmaların ehtimalını təyin edək (cədvəl 3.7)

$\hat{a}_1$, $\hat{b}_1$, $\hat{a}_2$, $\hat{b}_2$, $\hat{a}_3$, $\hat{b}_3$, $\hat{a}_4$ и $\hat{b}_4$ parametrlərin tapılan qiymətlərini (3.2) düsturuna qoymaqla müəyyənləşdiririk ki:

konfidensialliq üçün ($\beta_1 = 0.1$ olanda)

$$\hat{P}_2(z/t) = e^{-34.156e^{-0.3067\,t}\left[1-e^{-0.3067z}\right]} \qquad (3.7)$$

tamlıq üçün ($\beta_2 = 0.15$ olanda)

Cədvəl 3.6

İnformasiya təhlükəsizliyinin pozulmaları haqqında verilənlər

№	İllər	Təhlükəsizlik servislərinin pozulma sayı			
		Konfidensiallıq	*Tamlıq*	*Əlyetənlik*	*Avtorizasiya*
1	2001	7	134	154	263
2	2002	11	50	90	163
3	2003	3	84	64	100

$$\hat{P}_2(z/t) = e^{-497.056e^{-0.2856\cdot t}\left[1-e^{-0.2836z}\right]} \qquad (3.8)$$

əlyetənlik üçün ($\beta_1 = 0.2$ olanda)

$$\hat{P}_3(z/t) = e^{-440.321e^{-0.4265\cdot t}\left[1-e^{-0.4265z}\right]} \qquad (3.9)$$

avtorizasiya üçün ($\beta_1 = 0.18$ olanda)

$$\hat{P}_4(z/t) = e^{-712.771e^{-0.4656t}\left[1-e^{-0.46565z}\right]} \qquad (3.10)$$

Sonra (3.7)-(3.10) düsturlarından istifadə edərək hər bir təhlükəsizlik servisi üçün $\hat{P}_j(z/t)$, $j=\overline{1,4}$ ($z=1$ ay olanda) təyin edirik.

$$\hat{P}_1(z/t)=0.6970,\quad \hat{P}_2(z/t)=0.090,$$
$$\hat{P}_3(z/t)=0.020,\quad \hat{P}_4(z/t)=0.031$$

Cədvəl 3.7

Təhlükəsizlik servislərinin yığılmış cəminin qiyməti

№	İllər (t_i)	Təhlükəsizlik servislərinin yığılmış cəminin qiyməti			
		Konfidensiallıq $y_{i,1}$	*Tamlıq* $y_{i,2}$	*Əlyetənlik* $y_{i,3}$	*Avtorizasiya* $y_{i,4}$
1	2001	7	134	154	263
2	2002	18	184	244	426
3	2003	21	268	308	526

Növbəti addım olaraq, cədvəl 3.6-nın verilənlərindən istifadə edərək və (3.6) düsturu vasitəsi ilə M_S parametrinin, $L=2^4=16$ qiyməti təyin olunur. Sonra cədvəl qurulur və bu cədvələ M_S parametrinin L qiymətləri və (3.7)-(3.10) düsturlarını nəzərə almaq şərti ilə $\hat{P}_j(z,t)$, $j=\overline{1,4}$, qiymətləri daxil olunur (cədvəl 3.8).

Sonra isə "STATGRAPHICS" statistik paket proqramı və cədvəl 3.8-in verilənləri əsasında (3.5) bərabərliyinin reqressiya əmsallarının təyin edirik:

$$\alpha_0 = 0,\ \alpha_1 = 0.0268,\ \alpha_2 = 2.6511,\ \alpha_3 = 13.715,$$
$$\alpha_4 = 15.1097$$

Nəhayət, reqressiyanın əmsallarını (3.5) düsturunda yerinə qoyaraq, M_s üçün növbəti ifadəni almış olarıq:

$$M_s = 0.0268x_1 + 2.65111x_2 + 13.715x_3 + 15.1097x_4$$

Korporativ şəbəkənin informasiya təhlükəsizliyi pozulmasının ehtimalı isə:

$$Q_s = 1 - 0.0268x_1 - 2.65111x_2 - 13.715x_3 - 15.1097x_4$$

düsturu ilə təyin etmək mümkündür.

Cədvəl 3.8

M_s parametrinin qiymətlərinin hesablanması

No	Konfidensiallıq	Tamlıq	Əlyetənlik	Avtorizasiya	M_s
1.	0	0	0	0	0,0000
2.	0.6970	0	0	0	0,0187
3.	0	0.090	0	0	0,2386
4.	0	0	0.020	0	0,2743
5.	0	0	0	0.031	0,4684
6.	0.6970	0.090	0	0	0,2573
7.	0.6970	0	0.020	0	0,2930
8.	0.6970	0	0	0.031	0,4871
9.	0	0.090	0.020	0	0,5129
10.	0	0.090	0	0.031	0,7070

11.	0	0	0.020	0.031	0,7427
12.	0.6970	0.090	0.020	0	0,5316
13.	0.6970	0.090	0	0.031	0,7257
14.	0.6970	0	0.020	0.031	0,7614
15.	0	0.090	0.020	0.031	0,9813
16.	0.6970	0.090	0.020	0.031	1,0000

Təklif olunan metrikanın dəqiqliyinə təsir göstərən əsas faktorlar korporativ şəbəkələrdə olan informasiya təhlükəsizliyi pozulmalarının statistik verilənlərinin həcmi, baxılan təhlükəsizlik servislərinin sayı, şəbəkədə olan informasiya təhlükəsizliyi pozulmalarını, korporativ şəbəkəyə olan hücum və təhlükələri təhlükəsizlik servislərinə görə düzgün qruplaşdırmaqdan ibarətdir.

3.4. Korporativ şəbəkənin informasiya təhlükəsizliyinin qiymətləndirilməsi üçün qeyri-səlis model

Müasir informasiya texnologiyaları və telekommunikasiya vasitələrinin əsas məqsədlərindən biri də odur ki, bu vasitələr vahid bir informasiya məkanında çalışa bilsinlər. Bu məqsədin kəskin şəkildə meydana gəlməsinin əsas səbəblərindən biridə odur ki, müxtəlif proqram təminatı, əməliyyat sistemi və mühafizə sistemləri istehsalçılarının məhsulları vahid korporativ şəbəkə çərçivəsində bir-biri ilə bəzən konflikt yaradırlar. Bu sadəcə onların bir yerdə işləməsini əngəlləmir, həmçinin, korporativ şəbəkənin təhlükəsizlik sistemlərində boşluqlar da yaradır. Bədəməl şəxslər məhz belə boşluqlardan istifadə edərək korporativ şəbəkəyə müxtəlif miqyasda ziyan vura bilirlər. Verilənlərin mübadiləsi geniş həcmli və çox mürəkkəb şəbəkələr arası miqyasda baş verir və bunu idarə etmək həddindən artıq mürəkkəb məsələdir. Bununla eyni vaxta müxtəlif tipli informasiya təhlükəsizliyinin pozulması, məxfi olan və olmayan məlumatların ələ keçirilməsi kimi kompüter insidentlərinin də sayı durmadan artmaqdadır. Belə halda korporativ şəbəkənin

layihələndirilmə mərhələsində informasiya təhlükəsizliyi pozulmasının qiymətləndirilməsi çox vacib bir məsələdir.

Adətən praktikada korporativ şəbəkə layihələndirilən zaman təhlükəsizlik sisteminin bütün tərəflərini əhatə etmək mümkün olmur. Çünki hər bir təşkilatın özünə məxsus spesifik xüsusiyyətləri mövcuddur və korporativ şəbəkənin təhlükəsizlik sistemi sırf təşkilatın texniki tələblərinə uyğun olaraq layihələndirilir. Bu baxımdan hər bir təşkilata məxsus korporativ şəbəkənin mühafizə sistemi fərdi qaydada hazırlanıb, həyata keçirilir. Bir qayda olaraq mühafizəli korporativ şəbəkələrin layihələndirilmə mərhələsində ilkin verilənlər natamamlığı ilə xarakterizə olunurlar və bəzi hallarda mühafizəli korporativ şəbəkələrdə insidentlər haqqında heç bir məlumat olmur. Ona görə bu halda müsbət nəticə əldə etmək üçün qeyri-səlis çoxluqlar nəzəriyyəsindən istifadə etmək məqsədə uyğundur.

Fərz edək ki, $S = \{s_j\}, j = \overline{1,k}$ təhlükəsizlik servisləri çoxluğudur və onların hər birində yalnız bir informasiya təhlükəsizliyi funksiyası, yəni əlyetənlik, tamlıq və s. realizə olunub. Bu servislər korporativ şəbəkənin təhlükəsizlik sisteminin komponentləri sayılır. Korporativ şəbəkələrdə informasiya təhlükəsizliyini təmin edən servislərin realizə olunması, məsələn, 100% tamlıq funksiyasının qorunması hələ informasiyanın dəyişdirilmədən və ya ələ keçirilmədən tam qorunması demək deyildir. Həmişə sistemdə harasındasa zəif yerlər və ya boşluqlar mövcud olurlar və bunlarda informasiya təhlükəsizliyinin pozulmasına zəmin yaradırlar. Məhz bu səbəbdən korporativ şəbəkələrdə informasiya təhlükəsizliyinin pozulması ehtimalı iki komponentin cəmindən ibarətdir: realizə olunmamış servislərin təhlükəsizlik funksiyasının pozulması ehtimalı və realizə olunmuş servislərin təhlükəsizlik funksiyasının pozulması ehtimalı.

Bu vəziyyətdə birinci komponentin müəyyən olması heç bir problem törətmir. CERT təşkilatlarında korporativ şəbəkələrdə

realizə olunan ayrı-ayrı informasiya təhlükəsizliyi pozulmaları hallarının statistik verilənləri toplanır. Lakin, korporativ şəbəkələrdə realizə olunan ayrı-ayrı təhlükəsizlik funksiyalarının pozulmalarının statistik verilənləri əl yetməz olurlar. Bu verilənlər bütün hallarda məxfi olurlar. Ona görə də ikinci komponenti təyin etmək üçün, qeyri-səlis ehtimallardan istifadə olunur ki, onlarda öz növbəsində ekspert qiymətləndirilməsi nəticəsində əldə olunurlar. Bu halda informasiya təhlükəsizliyi pozulmasının ehtimalına qeyri-səlis çoxluq kimi baxılır və bunun aparıcısı 0-dan 1-ə qədər intervalda qiymətlər ala bilər. Ümumi halda bu aşağıdakı kimi ifadə oluna bilər:

$$\widetilde{P}_s = f(x_h) + \widetilde{\Phi}(x_g), \qquad (3.11)$$

burada - $\widetilde{P}_s$ - informasiya təhlükəsizliyi pozulmasının qeyri-səlis ehtimalıdır; x_h, x_g - müvafiq olaraq, korporativ şəbəkədə realizə olunan və olunmayan təhlükəsizlik servislərini xarakterizə edən parametrlərdir, $x_h \in A_h$, $x_g \in A_g$, $h, g \in J$; A_g, A_h - müvafiq olaraq, realizə olunan və olunmayan təhlükəsizlik servisləri çoxluğudur; J - təhlükəsizlik servislərinin indekslər çoxluğudur.

Onu nəzərə alsaq ki, korporativ şəbəkə layihələndirilən zaman ayrı-ayrı təhlükəsizlik servislərinin təsiri qeyri-müəyyən olduğundan, bu əlaqəni ümumi formada qeyri-səlis çoxdəyişənli xətti reqressiya şəklində yazmaq olar:

$$\widetilde{P}_s = \widetilde{D}_0 + \widetilde{D}_1 x_1 + \widetilde{D}_2 x_2 + \ldots + \widetilde{D}_k x_k \qquad (3.12)$$

burada $\widetilde{D}_0, \widetilde{D}_1, \ldots, \widetilde{D}_k$ - qeyri-səlis çoxdəyişənli xətti reqressiyanın qeyri-səlis əmsallarıdır; $x_1, x_2, \ldots, x_k$ - ayrı-ayrı servisləri xarakterizə edən parametrlərdir.

x_j, $j = \overline{1,k}$, $j \in J$ parametri əvəzinə etibarlılıq xarakteristikası istifadə etdiyimizdən, onda (3.12) düsturunun

konkret formasını müəyyən etmək üçün, ilk növbədə $(x_1, x_2, ..., x_k, \widetilde{P}_s)$ çoxluğunu təyin etməliyik. Təhlükəsizlik siyasətindən asılı olaraq, layihələndirilən zaman korporativ şəbəkədə müxtəlif təhlükəsizlik servisləri ixtiyari kombinasiyada realizə oluna bilərlər. Bu kombinasiyaların sayı $L = 2^k$, burada k – təhlükəsizlik servislərinin sayıdır. Təhlükəsizlik servislərinin hər bir realizə olunma variantı üçün, $x_1, x_2, ..., x_k$ verilənlər çoxluğunu formalaşdırmaq məqsədi ilə, aşağıdakı prosedura istifadə olunur:

$$x_j^{(l)} = \begin{cases} P_j(z/t), & \text{əgər } l \text{ variantında } j \text{ servisi realizə olunub,} \\ 0, & \text{əks halda} \end{cases} \qquad l = \overline{1, L}$$

Beləliklə, hər bir realizə olunmuş variant üçün $(x_1, x_2, ..., x_k)_l$, $l = \overline{1, L}$ tipli verilənlər çoxluğu almış oluruq.

Korporativ şəbəkədə realizə olunmayan servislərin təhlükəsizlik funksiyasının pozulması ehtimalını hər bir variant üçün müəyyən olunmasında, biz CERT təşkilatlarda olan statistik verilənlərdən istifadə edirik. Onda l variantı üçün layihələndiriləcək korporativ şəbəkədə realizə olunan təhlükəsizlik servisini belə təyin edirik:

$$p_1^{(l)} = \frac{\sum_{g \in A_l} y_{n,g}}{\frac{k}{\sum_{j=1} y_{n,j}}}, \quad g \in J, l = \overline{1, L}, \qquad (3.13)$$

burada A_l - l-ci variantda realizə olunmamış təhlükəsizlik servisləri çoxluğudur; $y_{n,j}$ - t_n anına olan j servisinin təhlükəsizlik funksiyası pozulmaları sayının yığılmış cəmidir;

$y_{n,g}$- t_n anına olan g servisinin təhlükəsizlik funksiyası pozulmaları sayının yığılmış cəmidir.

$\widetilde{p}_{2,j}$ ilə korporativ şəbəkədə realizə olunan j servisinin təhlükəsizlik funksiyası pozulmasının qeyri-səlis ehtimalını işarə edək.

$\widetilde{p}_{2,j}$ parametrin qiyməti ekspert qiymətləndirilməsi əsasında müəyyən olunur. Bu halda qeyri-səlis ehtimallar linqvistik anlayışlar kimi, $p_{2,j} \rightarrow [p^0_{2,j}, p^-_{2.j}, p^+_{2,j}]$ qiymətinə yaxın korporativ şəbəkədə realizə olunan j servisinin təhlükəsizlik funksiyasının pozulmaları ehtimalı şəklində formalaşır. Burada $p^0_{2,j}$, korporativ şəbəkədə realizə olunan j servisinin təhlükəsizlik funksiyasının pozulmalarının qeyri-səlis ehtimalının orta qiymətidir; $p^-_{2.j}, p^+_{2,j}$ - müvafiq olaraq $p_{2,j}$ parametrinin sol və sağ sərhədləridir.

Onda qeyri-səlis ədədlər üzərində qaydalara uyğun olaraq arifmetik əməliyyatları yerinə yetirərək, realizə olunan təhlükəsizlik servislərin l variantı üçün:

$$\widetilde{p}_2^{(l)} = \prod_{g \in A^{(l)}} \widetilde{p}_{2,g} = \left(\prod_{g \in A^{(l)}} p^-_{2,g}, \prod_{g \in A^{(l)}} p^0_{2,g}, \prod_{g \in A^{(l)}} p^+_{2,g} \right),$$

$$g \in J,\ l = \overline{1, L} \qquad (3.14)$$

ifadəni almış oluruq.

Burada $A^{(l)}$ - l-ci variantda realizə olunmuş təhlükəsizlik servisləri çoxluğudur.

$p_1^{(l)}$ və $\widetilde{p}_2^{(l)}$ ehtimalları asılı olmadıqları üçün, l-ci variantda realizə olunmuş təhlükəsizlik servisləri korporativ şəbəkənin informasiya təhlükəsizliyi pozulmalarının ehtimalı aşağıdakı kimi təyin olunur:

$$\widetilde{P}_s^{(l)} = (p_2^-, p_2^0, p_2^+) + q_1^{(l)}(1 - p_2^+, 1 - p_2^0, 1 - p_2^-),$$

$$l = \overline{1,L} \qquad (3.15)$$

burada, $q_1^{(l)} = 1 - p_1^{(l)}$.

Beləliklə, $(x_1, x_2, ..., x_k, \widetilde{P}_s)_l$, $l = \overline{1,L}$ tipli verilənlər çoxluğunu təyin etmiş oluruq və bunlar da öz növbəsində (3.12) tənliyində olan qeyri-səlis çoxdəyişənli xətti reqressiyanın əmsallarını təyin etmək üçün istifadə olunur. Bu halda ardıcıl olaraq $(x_1, x_2, ..., x_k, p_s^-)_l$, $(x_1, x_2, ..., x_k, p_s^0)_l$ və $(x_1, x_2, ..., x_k, p_s^+)_l$ tipli verilənlər çoxluğu vasitəsi ilə çoxdəyişənli xətti reqressiyanın əmsallarını $D_j = (d_j^-, d_j^0, d_j^+)$ formada təyin edirik.

Tapılan reqressiya əmsallarının qiymətlərini (3.12) düsturunda nəzərə alsaq, korporativ şəbəkənin informasiya təhlükəsizliyini qiymətləndirmək üçün ədədi metrikanı əldə etmiş oluruq:

$$\widetilde{P}_s = (d_0^-, d_0^0, d_0^+) + (d_1^-, d_1^0, d_1^+)x_1 + ... + (d_n^-, d_n^0, d_n^+)x_n \qquad (3.16)$$

Nəticələri aprobasiya etmək üçün növbəti misala diqqət yetirək. JANET/CC təşkilatında olan statistik verilənləri 4 təhlükəsizlik servisləri üzrə, yəni, konfidensiallıq, tamlıq, əlyetənlik və avtorizasiya siniflərinə bölək (cədvəl 3.6).

Sonra 3.6 cədvəlinin verilənləri əsasında və (3.4) tənliklər sisteminindən istifadə edərək, $\hat{a}_j$ və $\hat{b}_j$, $j = \overline{1,4}$, məchul parametrlərini hər bir servisə görə təyin etməyə başlayırıq (cədvəl 3.9). $\hat{a}_j$ və $\hat{b}_j$, $j = \overline{1,4}$, parametrlərinin tapılmış qiymətlərini (3.2) düsturuna $\beta_1 = 0.1$, $\beta_2 = 0.15$, $\beta_3 = 0.2$, $\beta_4 = 0.18$

olanda və $z = 1$ a y olduqda hər bir təhlükəsizlik servisi üçün dəqiq qiymət almış oluruq:

$$\hat{P}_1(z/t) = 0.697, \quad \hat{P}_2(z/t) = 0.090,$$

$$\hat{P}_3(z/t) = 0.020, \quad \hat{P}_4(z/t) = 0.031.$$

Bu verilənlər cədvəl 3.10-da göstərilmişdir.

Korporativ şəbəkələrdə servislər realizə olunan halda konfidensialliq, tamlıq, əlyetənlik və avtorizasiya servislərinin təhlükəsizlik funksiyası pozulmasının qeyri-səlis ehtimalını əvvəlcədən

$$\tilde{p}_{2,1} = (0.005, 0.01, 0.015),$$

$$\tilde{p}_{2,2} = (0.01, 0.02, 0.03),$$

$$\tilde{p}_{2,3} = (0.025, 0.05, 0.075),$$

$$\tilde{p}_{2,4} = (0.01, 0.03, 0.05)$$

şəkildə müəyyən edək. Onda (3.13)-(3.15) düsturlarına əsasən təhlükəsizlik servislərinin hər bir realizə olunma variantı üçün, $\tilde{P}_s = (p_s^-, p_s^0, p_s^+)$ parametrinin qiymətini təyin edirik.

Cədvəl 3.9

$\hat{a}_j$ və $\hat{b}_j$ parametrlərin qiymətləri

Konfidensiallıq		**Tamlıq**		**Əlyetənlik**		**Avtorizasiya**	
$\hat{a}_1$	$\hat{b}_1$	$\hat{a}_2$	$\hat{b}_2$	$\hat{a}_3$	$\hat{b}_3$	$\hat{a}_4$	$\hat{b}_4$
30.740	0.340	397.645	0.333	352.257	0.533	584.472	0.567

Cədvəl 3.10

Çoxdəyişənli qeyri-səlis reqressiyanın əmsallarının təyin etmək üçün verilənlər

No	Konfi-densialıq	Tamlıq	Əl-çatanlıq	Avto-rizasiya	$\tilde{P}_s = (p_s^-, p_s^0, p_s^+)$
1.	0	0	0	0	(0,0000, 1.0000, 0,0000)
2.	0.6970	0	0	0	(0.9814, 0.9815, 0.9816)
3.	0	0.090	0	0	(0.7638, 0.7662, 0.7686)
4.	0	0	0.020	0	(0.7325, 0.7394, 0.7463)
5.	0	0	0	0.031	(0.5387, 0.5457, 0.5527)
6.	0.6970	0.090	0	0	(0.7466, 0.7504, 0.7542)
7.	0.6970	0	0.020	0	(0.7157, 0.7244, 07331)
8.	0.6970	0	0	0.031	(0.5226, 0.5322, 0.5418)
9.	0	0.090	0.020	0	(0.5049, 0.5225, 0.5401)
10.	0	0.090	0	0.031	(0.3105, 0.3279, 0.3453)
11.	0	0	0.020	0.031	(0.2867, 0.3156, 0.3345)
12.	0.6970	0.090	0.020	0	(0.4894, 0.5100, 0.5306)
13.	0.6970	0.090	0	0.031	(0.2858, 0.3170, 0.3392)
14.	0.6970	0	0.020	0.031	(0.2724, 0.3054, 0.3384)
15	0	0.090	0.020	0.031	(0.0670, 0.1138, 0.1616)
16	0.6970	0.090	0.020	0.031	(0.0540, 0.1060, 0.1580)

Həmçinin bu verilənlər cədvəl 3.10-da göstərilmişdir. STATGRAPHICS Plus 5.0 statistik paket proqramının köməkliyi ilə $\tilde{D}_j = (d_j^-, d_j^0, d^+)$, $j = \overline{1,4}$ qeyri-səlis əmsallarını təyin edək

$$\tilde{D}_0 = (0.9728, 0.9817, 0.9906),$$

$$\tilde{D}_1 = (-0.0226, -0.0187, -0.0146),$$

$$\tilde{D}_2 = (-2.5250, -2.4033, -2.2816),$$

$$\tilde{D}_3 = (-12.7301, -11.7738, -10.8175),$$

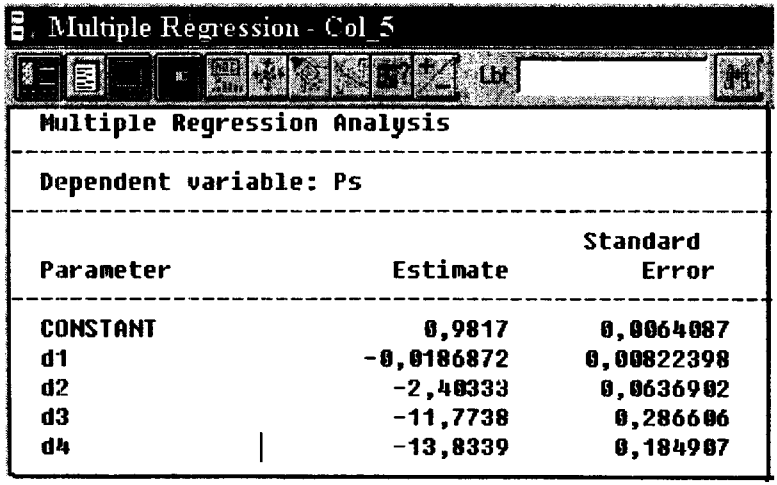
$$\tilde{D}_4 = (-14.4661, -13.8339, -13.2037).$$

Nümunə olaraq şəkil 3.6-da SATGRAPHİCS statistik proqram paketi vasitəsi ilə $(x_1, x_2, ..., x_k, p_s^0)$ verilənləri üçün reqressiya əmsallarının hesablanma nəticələri verilmişdir.

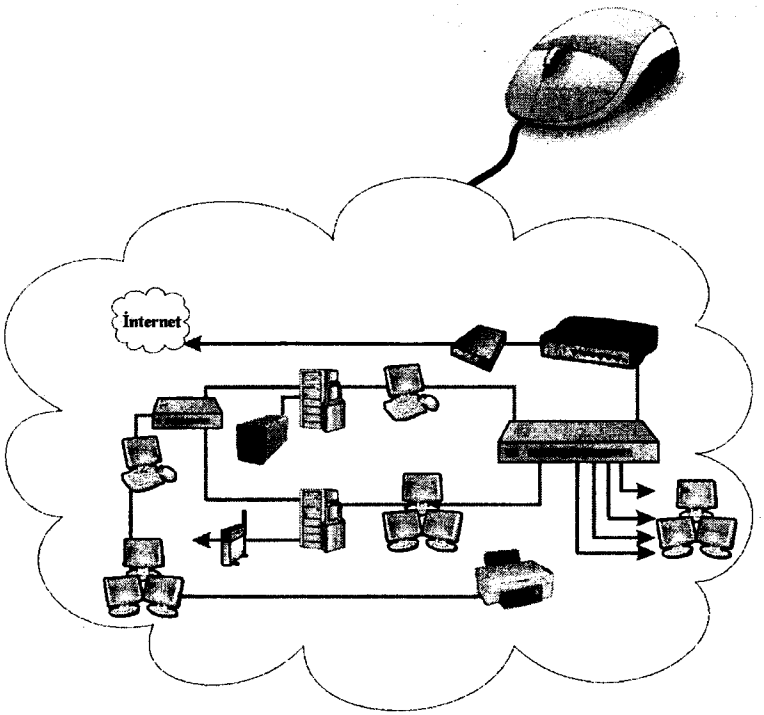
Nəhayət, reqressiyanın qeyri-səlis əmsallarını (3.12) düsturunda yerinə qoyaraq, $\tilde{P}_s$ üçün növbəti ifadəni almış olarıq:

$$\begin{aligned}\tilde{P}_s = {} & (0.9728, 0.9817, 0.9906) + (-0.0226, -0.0187, \\ & -0.0146)x_1 + (-2.5250, -2.4033, -2.2816)x_2 + \\ & + (-12.7301, -11.7738, -10.8175)x_3 + \\ & + (-14.4661, -13.8339, -13.2037)x_4\end{aligned}$$

Beləliklə, alınan nəticələr onu göstərir ki, ilkin verilənlərin tam olmadığı (və ya qeyri-dəqiq, rəqəmlə ifadə oluna bilməyən) zaman, qeyri-səlis çoxluqlar nəzəriyyəsi vasitəsi ilə layihələndirilmə mərhələsində korporativ şəbəkənin informasiya təhlükəsizliyini qiymətləndirmək mümkündür.



Şəkil 3.6 Çoxdəyişənli qeyri-səlis reqressiyanın əmsallarının hesablanmasından bir fraqment.



FƏSİL 4

SERVERİN İDARƏ OLUNMASI VƏ SERVİSLƏRİN TƏŞKİLİ

SERVERİN İDARƏ OLUNMASI VƏ SERVİSLƏRİN TƏŞKİLİ

- Sistem jurnalları
- Komanda sətri
- Kompüterin idarə olunması
- Active Directory və onun funksiyaları
- Active Directory və təhlükəsizlik
- Active Directory xidmətinin replikasiyası
- Active Directory xidmətinin istifadəçiləri
- Sistemin məhsuldarlığının artırılmasının əlavə vasitələri
- Məhsuldarlıq və miqyaslılıq
- Konfiqurasiyanın idarə olunması

Fəsil 4. SERVERİN İDARƏ OLUNMASI VƏ SERVİSLƏRİN TƏŞKİLİ

Korporativ şəbəkələrdə olan müxtəlif təyinatlı serverlərin (Active Directory server, Veb server, Fayl server, Poçt server, Print server və s.) düzgün idarə olunması və servislərin məntiqi ardıcıllıqla işə salınması nəticə etibarı ilə şəbəkənin işləmə keyfiyyətini və təhlükəsizlik kimi vacib problemləri həll etmiş olur. Korporativ şəbəkəni düzgün idarə etmək məqsədi ilə şəbəkə administratorlarının bir sıra vacib sistem vasitələrdən istifadəsi qaçılmazdır. Bu vasitələrdən sistem jurnalları, komanda sətri, Active Directory, sistemin məhsuldarlığını artırmaq üçün istifadə olunan əlavə vasitələri göstərmək olar.

4.1 Sistem jurnalları

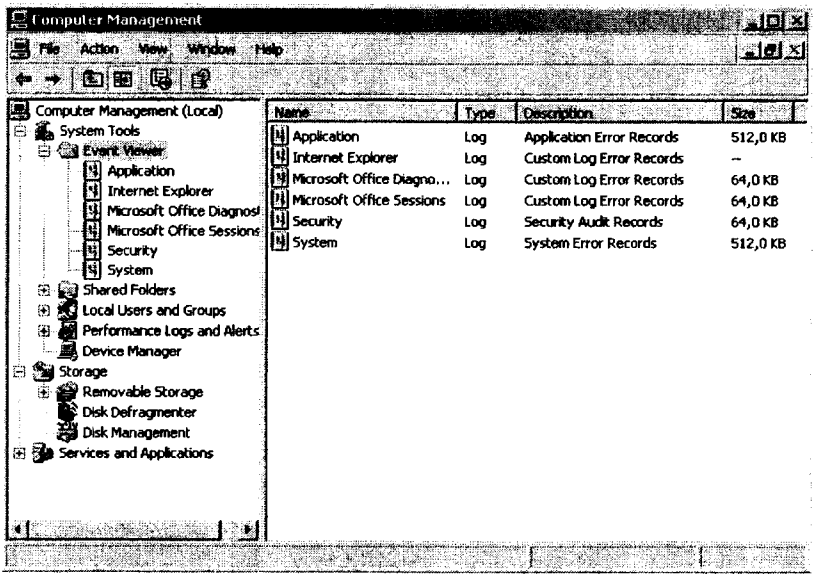
Korporativ şəbəkənin administratorunun əsas iş prinsiplərini müəyyən etdikdən sonra artıq şəxsi praktikada bir sıra məsələlərin həllinə və idarəetmə üslublarına baxmaq olar. Demək olar ki, korporativ şəbəkələrin bir çox administratorlarının gündəlik formasında olan jurnalları mövcuddur. Bu jurnalda administrator tərəfindən lazım sayılan və həyata keçirilən bütün hadisələr qeydə alınır. Ancaq praktikada tez-tez rast gəlinən problemlərdən biri də odur ki, bu jurnalda olan yazılar növbəti sapma zamanı qərar verməyə tam bəs etməsin. Odur ki, ixtiyari serverin əməliyyat sisteminin daxilində baş verən bütün hadisələri və serverin işləməsində əngəl törədən, sistem proqram təminatında sapmaların yaranma səbəbi olan hadisələr toplusunu qeydə alan bir sistem mövcuddur. Buna əməliyyat sisteminin "sistem jurnalı" deyilir. Bu sistem jurnalın əmələ gəlmiş hər hansı bir problemin kökünə çıxmaq üçün administratorun şəxsən yazdığı jurnala böyük dəstəyi ola bilər. Hər bir sistem jurnal hansı hadisələri qeydə almaq üçün nəzərdə tutulubsa, məhz o hadisələrin baş vermə tarixini özündə cəmləşdirir. Bu jurnalların yazılarını ilk baxışdan oxumaq çətin

olur. Çünki burada informasiya həddindən artıq müfəssəl şəkildə verilir və sistemin bütün xirdalıqları nəzərə çatdırılır. Əgər hadisə hər hansı bir səhv haqqında məlumat daşıyırsa və bu səhv məlum səhvlər siyahısındandırsa, onda onun haqqında qısa məlumat və identifikator göstərilir. Göstərilmiş identifikator əsasında Microsoft biliklər bazasında ona uyğun izahı tapmaq mümkündür. Amma praktikada elə hallara rast gəlinir ki, onların haqqında heç bir məlumat əldə etmək mümkün olmur. Baxmayaraq ki, Microsoft öz biliklər bazasını əməliyyat sistemləri və proqram təminatlarının sapmaları və ya işləmə zamanı səhvlərin aşkar olunması tipli informasiya ilə aktiv şəkildə müntəzəm genişləndirir, amma yenə də məlum olmayan səhvlər və sapmalar öz mövcudluğunu göstərir. Bunun əsas səbəbi kimi administratorun yanlış idarəetməsinin nəticəsində meydana gələn səhvləri göstərmək olar. Bu tip səhvlərin istehsalçı tərəfindən qabaqcadan nəzərə alına bilinməsi qeyri-mümkündür. Amma buna baxmayaraq sistem jurnalda bütün yazılar öz əksini tapır və öz növbəsində yaranmış problemi lokallaşdırmaq və ya aradan götürməyə kömək edir. Sistem jurnallar yalnız server əməliyyat sistemində deyil artıq bütün müasir işçi stansiyalarına məxsus əməliyyat sistemində də mövcuddur. Çünki serverdə olan problemlər işçi stansiyalarından qaynaqlana bilər. MS Windows NT 4.0 əməliyyat sistemindən başlayaraq bütün Windows ailəsinin əməliyyat sistemində sistem jurnala "Event Viewer" (Hadisələrə baxış) bölməsindən baxmaq mümkündür (şəkil 4.1).

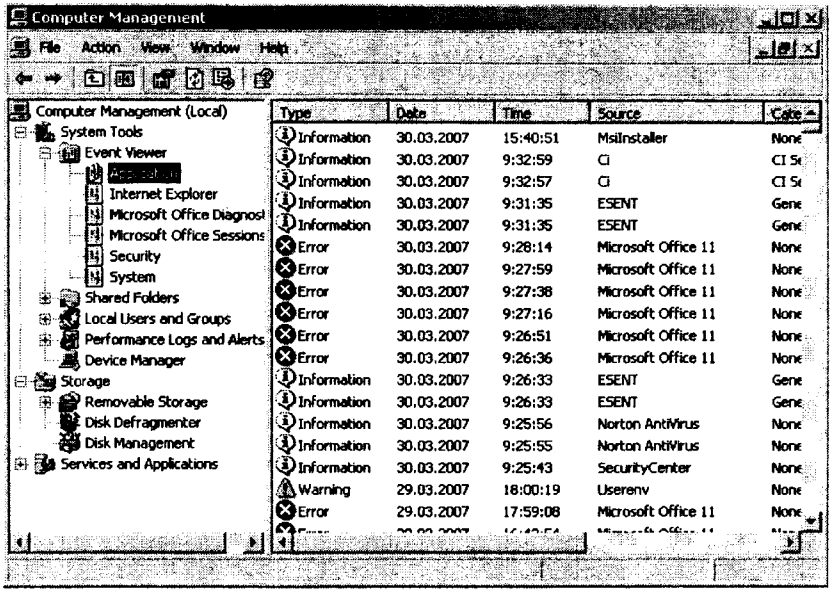
İşçi stansiyalarına məxsus əməliyyat sisteminində avtomatik olaraq üç sistem jurnalı fəaliyyət göstərir. Bunlar:

- sistemin jurnalı – System,
- proqram təminatı jurnalı – Application
- təhlükəsizlik jurnalı – Security.

Bu jurnalları siyahıdan seçməklə onların tərkibinə baxmaq mümkündür. Açılmış pəncərənin sağ tərəfində cari jurnalın məlumatlar siyahısını görmək olar (şəkil 4.2).



Şəkil 4.1 "Event Viewer" pəncərəsində hadisələrin siyahısı

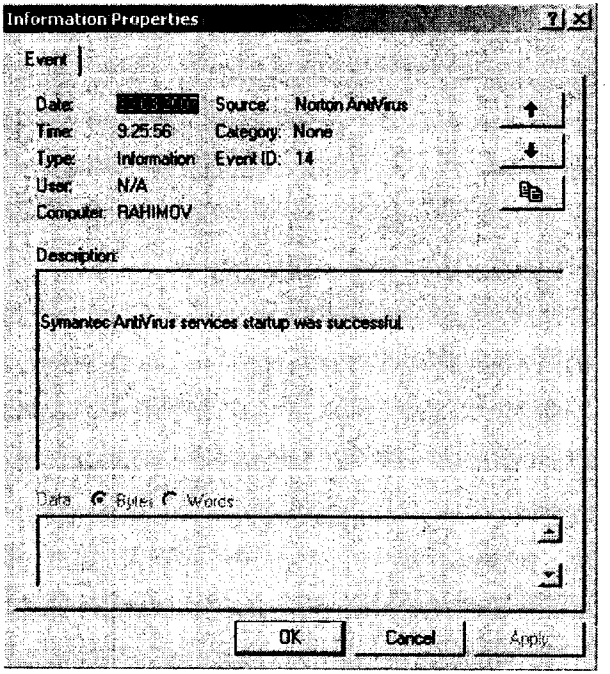


Şəkil 4.2 "Event Viewer" pəncərəsində "Application" bəndi

Məlumatların üç tipi vardır:

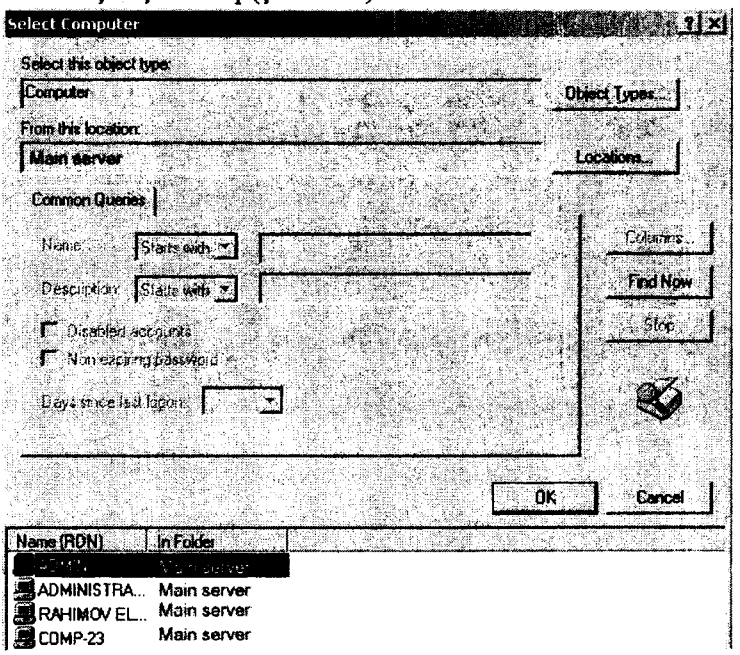
- Bildiriş (İnformation);
- Xəbərdarlıq (Warning);
- Səhvlər (Error).

İxtiyari məlumata baxmaq üçün onun xassələr bəndinə baxmaq kifayətdir (şəkil 4.3). Hadisələrin xassələr pəncərəsində, hadisələr haqqında məlumatı nəzərdən keçirmək mümkündür. Lazım gələrsə hadisə haqqında daha geniş və ətraflı məlumatı burada olan link vasitəsi ilə Microsoft biliklər bazasına qoşularaq, əldə etmək olar. Burada olan və üzərində ox işarəli düymələr vasitəsi ilə cari jurnala məxsus bir hadisədən digər hadisəyə keçid təmin olunur. Serverə məxsus əməliyyat sistemində, sistem jurnalların sayı çoxdur. Korporativ şəbəkənin fasiləsiz və qüsursuz işləməsini təmin edən servislərin hər birinin öz şəxsi jurnalı mövcuddur.



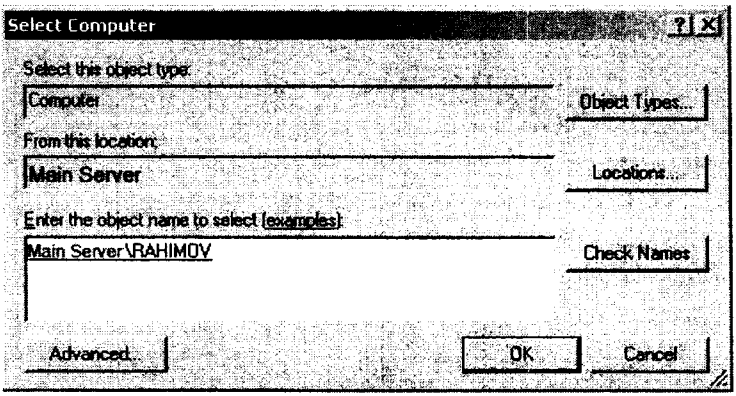
Şəkil 4.3 Hadisələrin xassələri pəncərəsi

Korporativ şəbəkənin serverində hadisələr jurnalına baxmaq üçün yuxarıda qeyd etdiyimiz qaydaya əsasən lazım olan sistem jurnalı açıb istədiyimiz məlumatı əldə edə bilərik. Digər tərəfdən korporativ şəbəkənin müxtəlif işçi stansiyalarının sistem jurnallarına bir neçə pəncərə şəkilində bir kompüterdə, məsələn idarəetmə serverində baxmaq daha məqsədə uyğundur. MS Windows XP əməliyyat sistemində çalışan ixtiyari kompüterin sistem jurnalına korporativ şəbəkənin hər hansı bir digər işçi stansiyasından baxmaq mümkündür. İşçi stansiyanı şəbəkə üçün sazlayan zaman onun lokal administratorlar siyahısına domen administratoru daxil etmək lazımdır. "Event Viewer" bəndinin üzərinə gəlib yuxarı menyuda "Action" bəndində "Connect to another computer" bölməsini seçirik. Açılmış pəncərədə "Browse..." düyməsini basırıq. Növbəti açılmış pəncərədə isə "Advanced..." düyməsini basaraq, kompüter seçmək üçün pəncərəni açmış oluruq (şəkil 4.4).

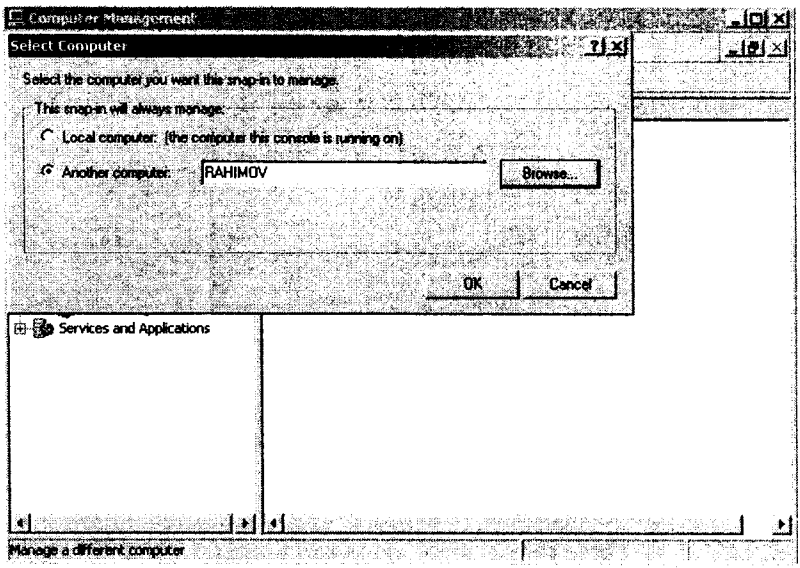


Şəkil 4.4 Kompüterin seçilməsi pəncərəsi

Burada hərfləri daxil etməklə və ya "Find" düyməsinin basmaqla kompüterlərin və serverlərin siyahısı ekrana çıxacaq və bu siyahıdan lazım olan serveri və ya kompüteri seçmək mümkündür. Açılmış cari pəncərədə harada ki, seçdiyimiz kompüterin adı görünür "OK" düyməsini basırıq (şəkil 4.5). Növbəti açılmış pəncərədə (şəkil 4.6) yenidən "OK" düyməsini basırıq.



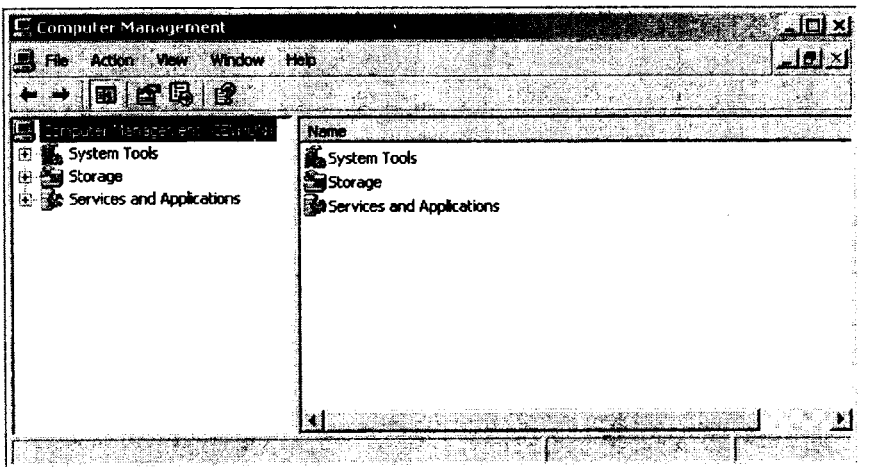
Şəkil 4.5 Kompüteri seçdikdən sonra açılan pəncərə



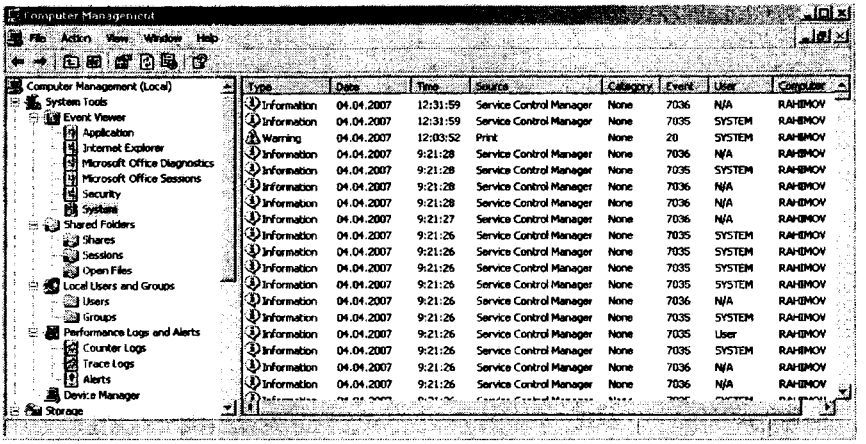
Şəkil 4.6 "OK" düyməsi ilə təsdiqləyəndən sonra açılan pəncərə

Əgər axtardığımız kompüterin adı dəqiq məlumdursa və heç bir şübhə doğurmursa, onda onun adını birbaşa olaraq "Select Computer" pəncərəsinin müvafiq yerinə daxil edirik. Bundan sonra artıq tanış olan "Computer Management" pəncərəsi seçdiyimiz kompüter üçün açılır (şəkil 4.7).

Korporativ şəbəkənin administratoru ixtiyari jurnalda müxtəlif yazılara baxa bilmək imkanına malikdir. (şəkil 4.8). Lakin praktikada belə hallarda mümkündür ki, korporativ şəbəkənin administratoru yalnız serverlərdə deyil, həmçinin ərazi baxımından onlarla kilometr uzaq məsafədə yerləşən işçi stansiyalarda da hadisələr jurnalına nəzarət edə bilər. Belə məsafədə yerləşən işçi stansiyalara qoşularaq administrator həmin kompüterlərə və serverlərə yaxınlaşmadan, yəni məsafədən və iş prosesi zamanı işçiləri öz kompüterlərindən ayırmadan, özünə lazım olan informasiyanı əldə etmək imkanına malikdir.



Şəkil 4.7 Serverdə olan hadisələrin siyahısı pəncərəsi



Şəkil 4.8 Sistemdə baş verən hadisələrin siyahısı

4.2 Komanda sətri

Hadisələr jurnalında hər bir məlumatın özünə məxsus tipi və identifikator kodu (ID) var. Hər bir identifikatora müəyyən hadisələr izahı uyğun gəlir. Hadisələr jurnallarını nəzərdən keçirərək, administrator hər hansı bir səhvin və ya digər hadisənin müntəzəm əmələ gəlməsinə nəzarət edə bilər. Lakin bir jurnalın bütün yazılarını nəzərdən keçirmək çox yorucu işdir. Hadisələr jurnalında olan yazıların sayı həddindən çox olur və eyni tipli yazıları müəyyən etmək üçün çoxlu vaxt sərf etmək lazımdır. Lakin MS Windows XP əməliyyat sistemi daxilində olan və VBScript proqramlaşdırma dilində yazılan sistem proqram, əvvəlcədən təyin olunmuş meyarlar əsasında, hadisələr jurnalının yazılarını süzgəcdən keçirməyə, hadisə haqqında məlumatın əmələ gəlməsi tarixi və vaxtını müəyyən etməyə imkan verir. Bu proqramın istifadəsindən sonra bütün lazımi yazıları tapmaq çox asanlaşır. Həmçinin bu proqram korporativ şəbəkədə və ya kompüterin sistemində yazıların yaranmasını və hadisələr arasında əlaqəni müəyyən etmək üçün istifadə olunur. Bu sistem proqramın adı "eventquery.vbs"-dir. Onu işə salmaq üçün "cmd" komanda

sətri proqramını işə salmaq lazımdır. Sonra isə komanda sətrində aşağıdakı əmri yazmaq lazımdır:

cscript c:\windows\system32\ eventquery.vbs /<parametrlər>.

Parametrlər kimi növbəti göstəriciləri daxil etmək olar:

- **/l** <"jurnalın adı"> – axtarışda olan jurnalı təyin edir;
- **/s** – bütün məlumatlar;
- **/r N** – axırıncı N hadisə;
- **/r -N** – ən köhnə N hadisə;
- **/r N-M** –N-dən M-ə qədər olan hadisələr;
- **/fi "id eq Q"** – Q identifikatorlu bütün hadisələr;
- **/fi "id nq Q"** – identifikatoru Q-yə bərabər olmayan bütün məlumatlar;
- **/fi "id ge Q"** – identifikatoru Q-yə bərabər və ya böyük olan bütün məlumatlar;
- **/fi "id i t Q"** – identifikatoru Q-dən kiçik olan bütün məlumatlar;
- parametrlər sətrində "**or**" operatorunu tətbiq etmək olar.

/fi əməliyyatı ilə başlayan parametrləri kombinə etmək olar. Korporativ şəbəkənin ixtiyari nöqtəsindən serverə giriş əldə etmək üçün növbəti parametrləri əlavə etmək olar:

/s systemname – serverin adını daxil edirik;

/u username – istifadəçinin adını daxil edirik;

/p password – giriş parolunu daxil edirik

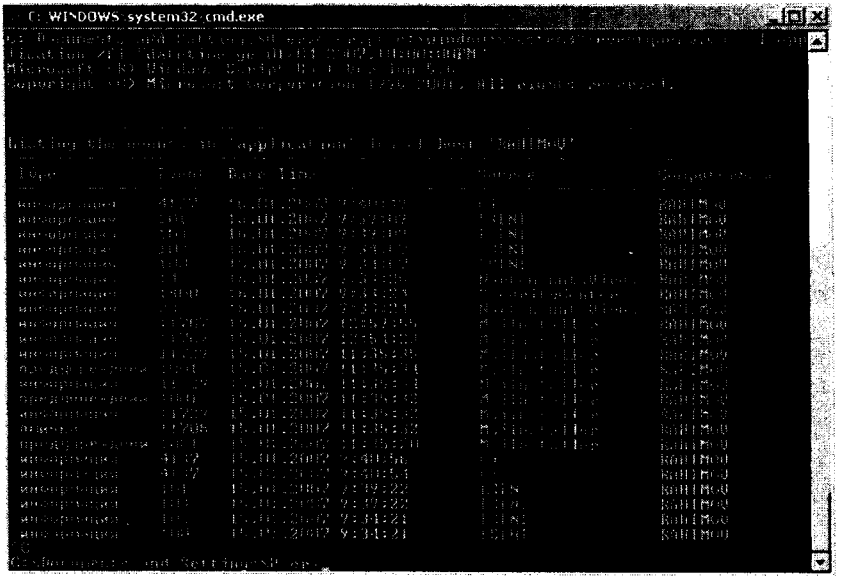
Məlumatları bir-birindən vergüllə ayrılmış vahid bir fayla yığılması üçün **/fo csv** parametrini əlavə etmək məqsədə uyğundur. Məlumatların həqiqətəndə bir fayla yığılması üçün, komanda sətrində adi qaydada, komandadan sonra ">" işarəsini qoymaq və faylın adını onun yerləşdiyi ünvanı ilə birlikdə tam şəkildə göstərmək lazımdır. Bütün adları və faylın ünvanlarını dırnaq arasında yazmaq vacibdir. ID identifikatorundan başqa bütün məlumatları tarix və vaxta görə (datetime); tipə görə (type); istifadəçiyə görə (user); kompüterə görə (computer); məlumatın

mənbəyinə görə (source); məlumatların kateqoriyasına görə (category) süzmək mümkündür.

Şəkil 4.9 –da komanda sətri pəncərəsində

cscript c:\windows\system32\ eventquery.vbs /l application /fi "datetime ge 01/04/2007,10:00:00PM"

əməliyyatı yerinə yetirlir və lokal jurnalların bütün məlumatlarını ekrana çıxarır. Bu komanda sətrinə **/fo csv > c:\err.csv** əmrini əlavə etsək, onda əmrin yerinə yetirilməsinin nəticəsi **C:** diskində "err.csv" faylına toplanacaqdır. Fayl DOS kodlaşmasında yaradılacaq.



Şəkil 4.9 "eventquery" əmri

Əslində belə uzun əmrləri daxil etmək heçdə rahat bir iş deyil. Lakin elə paket və komanda faylları var ki, onlarda belə uzun əmrləri əvvəlcədən yazıb, yadda saxlayıb və lazım olduqda birbaşa istifadə etmək olur. Əgər əmr düzgün yazılmayıbsa, ekranda dərhal səhv və onun düzgün yazılış qaydası haqqında məlumat əmələ gəlir. Sistem proqramı olan "eventquery.vbs" haqqında əlavə məlumatı özündə cəmləyən faylı mətn

redaktorlarının birində açıb onun proqram kodunu analiz edərək, əldə etmək olar. Bu sistem proqram vasitəsi adətən administratorlar tərəfindən çox istifadə olur.

Səhvlər haqqında məlumat. Müxtəlif səhvlər haqqında məlumat yalnız hadisələr jurnalında olmurlar. Bu həmçinin məsələn, əməliyyat sistemində hər hansı bir proqramın quraşdırılması, işləyərkən sapmalar və ya müxtəlif resurslara giriş əldə edilən zaman baş verə bilən səhvlər də ola bilər. Əlbəttə ki, səhvlərin əmələ gəlməsinin bütün səbəblərini sadalamaq və onların izahını vermək mümkün deyil. Bəzən praktikada sistem tərəfindən elə bir səhv haqqında məlumat verilir ki, hətta çox təcrübəli istifadəçi belə bu səhv qarşısında texniki cəhətdən aciz qalır. Belə hallarda vəziyyətdən çıxış kimi başa düşülməyən məlumatları izah edən, həcmcə kiçik olan sistem proqramlardan istifadə etmək məqsədə uyğundur. İndi isə bu silsilədən olan bir neçə sistem proqrama nümunə şəklində baxaq:

Exchange Server Error Code Look-up. Faylın adı – "err.exe", və komanda sətrindən işləyən sistem proqram olan "Exchange Server Error Code Look-up" (Exchange serverin səhvlərinin kodlarına baxış). "Exchange Server" proqramı və köməkçi vasitələr istifadə olunmadan informasiya mübadiləsinin serverində səhvlər mənbəyinin tapılması qeyri-mümkündür. Bu vasitə MS Windows XP/2000/2003 əməliyyat sistemində heç bir maneə olmadan işləyir. Məlumdur ki, proqram təminatlarının yerinə yetirilməsi zamanı əmələ gələn səhvlər haqqında məlumat, ancaq istehsalçı təşkilatın proqramçılarının bu tip səhvlərin ekrana çıxmasını nəzərə aldıqlarına görə dərhal ekranda təsvir olunur. Əgər səhvin kodu məlumdursa, onda onun müvafiq izahı da mövcuddur. Lakin belə hallarda mövcuddur ki, eyni səhvlər müxtəlif əməliyyat sistemində ayrı-ayrı kodlarla işarələnir. Bu səbəbdən cari sistemdə konkret səhv haqqında geniş məlumat almaq üçün "Exchange Server Error Code Look-up" sistem proqramını istifadə etmək məqsədə uyğundur.

İstifadə qaydası:

err <qiymət> [qiymət] [qiymət] . . .

burada <qiymət > aşağıda olan ifadələrin qiymətlərinin birinə bərabər olmalıdır:

* onaltılıq (0x54f);
* aydın olmayan onaltılıq (54f);
* tək saylardan olmayan (1359) – proqram 0x1359 və 1359 qiymətini axtaracaq;
* səhv haqqında məlumatın dəqiq sətri **(ERROR_INTERNAL_ERROR)**;
* altsətir (**INTERNAL_ERROR**).

Proqram səhv haqqında bütün məlumatları sistemin ***.h** (C:\WINDOWS\system32\) genişlənməsi ilə olan və başlıq adlanan fayllarında axtarır.

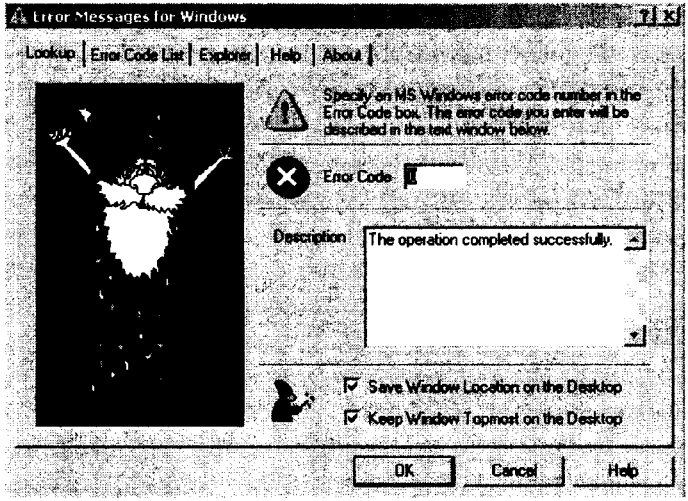
İndi isə **err 0x5dc** əmrinin yerinə yetirilməsinə baxaq, bu isə öz növbəsində 1500 nömrəli səhvin axtarışına uyğun gəlir. Ekrana aşağıda göstərilən məlumat çıxarılacaq:

 # for hex 0x5dc / decimal 1500:
ecScottBriggsMin ec.h
SCEEVENT_INFO_BACKUP_SECURITY uevents.me
 # Security configuration was backed up to %1.
ERROR_EVENTLOG_FILE_CORRUPT winerror.h
 # The event log file is corrupted.
 # 3 matches found for "0x5dc"

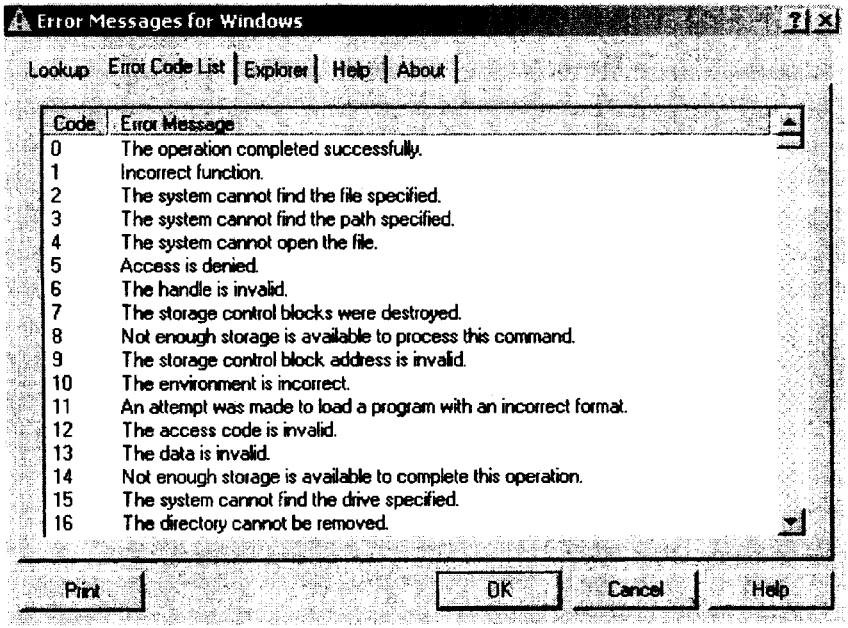
Yuxarıda nümunə kimi göstərilən sətirlərdən görmək olar ki, bu səhvin realizə olunması zamanı hadisələrin loq faylı zədələnmişdir (The event log file is corrupted).

Error Messages for Windows. "Error Messages for Windows" sistem proqram MS Windows əməliyyat sistemində işləyir. Bu sistem proqram "Shellapi.dll" kitabxanasında olan məlumatdan istifadə edərək, sistemi daha yaxşı anlamağa imkan yaradır. Bu sistem proqram vasitəsi istifadədə o qədər rahat və

başa düşüləndir ki, şəkil 4.10 və şəkil 4.11-ə baxmaqla onun haqqında tam təsəvvür yaranır.



Şəkil 4.10 Konkret səhv haqqında məlumat pəncərəsi



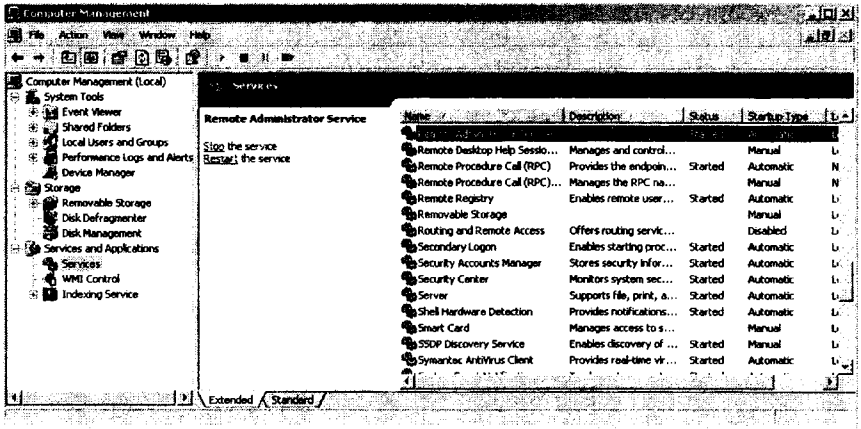
Şəkil 4.11 "Error Messages for Windows" proqramı

4.3 Kompüterin idarə olunması

Bu bölmədə biz məsafədə yerləşən sistemlərin idarə olunmasının bəzi vasitələrini və əsasən serverləri nəzərdən keçirəcəyik. Bu idarəetmə vasitələrini məsafədə olan işçi stansiyaların idarə olunmasında da tətbiq etmək olar. MS Windows əməliyyat sisteminin daxilində olan "Computer Management" (kompüterin idarə olunması) vasitəsi yalnız lokal kompüteri deyil, həm də məsafədə yerləşən kompüteri idarə etməyə imkan verir. Lokal idarəetmənin bütün imkanlarını şəbəkəyə şamil etmək olmur. Lakin tətbiq edilməsi mümkün olan funksiyalar korporativ şəbəkənin administratorun işini xeyli rahatlaşdırır. Bu rahatçılıqdan istifadə etmək üçün domen administratoru adından "Computer Management" bəndini açmaq və sonra yuxarı menyuda "Action" bölməsində "Connect to another computer" bəndini seçmək kifayətdir. Əgər korporativ şəbəkənin digər kompüterinə qoşulma alınmırsa, onda qoşulmaq istəyən istifadəçi məsafədə olan kompüterin administratorlar siyahısına daxil deyildir. Belə halda ancaq bu işçi stansiyaya fiziki yaxınlaşmaq və orada lazımi istifadəçini domen administratoru kimi sistemə daxil etmək lazım olacaqdır.

Əgər işçi stansiyanı idarə etmək tələb olunmursa və yalnız ona qoşulmaq lazımdırsa, yenə də cari istifadəçini domen administratoru kimi sistemə tanıtmaq lazımdır. Bu əməliyyatı etdikdən sonra artıq istifadəçinin korporativ şəbəkədə mobilliyi təmin olunur. Beləliklə "Computer Management" vasitəsini domen administratoru adından açırıq və korporativ şəbəkənin digər kompüterinə qoşuluruq. Açılmış pəncərənin sol tərəfində obyektlər kataloqunu açıb orada "Services" bəndini seçirik (şəkil 4.12). Məhz bu bölmə kompüterlərin idarə edilməsində administratorların marağını cəlb edən məqamlardandır. Müxtəlif xidmətləri yerinə yetirmək üçün əməliyyat sistemində olan və istifadəçilər tərəfindən əlavə yazılan bir sıra proqramlar işə salınır. Amma bütün xidmətlərin eyni zamanda işləməsinə heç bir ehtiyac

yoxdur. Məsələn, az istifadə olunan faks xidməti və bir sıra digər xidmətləri dayandırmaq olar, bu isə öz növbəsində işçi stansiyanın gündəlik iş rejimində onun resurslarına qənaət etmək deməkdir. Məsafədən idarə etmək proqramlarının içərisində ən məşhuru olan "Radmin" proqramını göstərmək olar. Bu proqram özü də xidmətlər siyahısında olur. Korporativ şəbəkənin administratoru məsafədə olan işçi stansiyasının resurslarına qənaət etmək və onun təhlükəsizliyini icazəsiz girişlərdən qorumaq məqsədi ilə bu xidməti lazım olduqda işə sala bilər.



Şəkil 4.12 Computer Management pəncərəsi

Lokal giriş zamanında olduğu kimi administrator əməliyyat sisteminin xidmətlərini işə salar, dayandırar və digər əməliyyatlar həyata keçirə bilər. Məsafədə yerləşən istifadəçilərin qeydiyyat yazılarını da analoji qaydada idarə etmək olar. Bu əməliyyatı "Computer Management" vasitəsinin "System Tools" bəndini seçməklə reallaşdırmaq olar. Adətən praktikada korporativ şəbəkənin ilk və əsas serverini Active Directory vasitəsinin xidməti kataloqlarını tətbiq etmək üçün nəzərdə tuturlar. Məhz bu səbəbdən lokal istifadəçilər korporativ şəbəkənin digər serverlərində və ya köməkçi serverlərində yerləşdirilir. Belə olan halda lokal işçi stansiyalardan Active Directory vasitəsinin

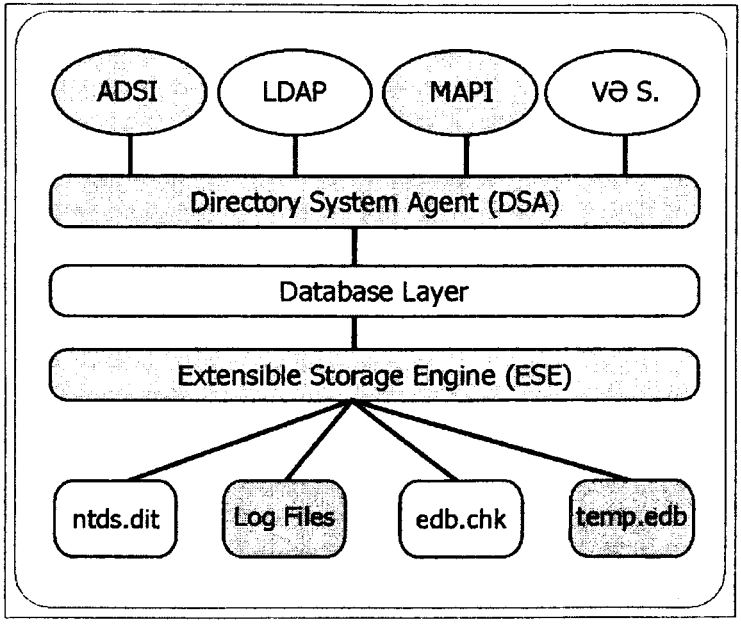
istifadəçilərinin qeydiyyat yazılarına əlavə proqram vasitəsi olmadan giriş əldə etmək mümkün olmur. Odur ki, əlavə proqram vasitələrini server üçün nəzərdə tutulmuş əməliyyat sisteminin distributiv disklərində tapmaq olar. Məsələn, server üçün nəzərdə tutulmuş əməliyyat sisteminin distributiv disklərində "i386" qovluğunun içində "adminpak.msi" faylını tapıb onu korporativ şəbəkənin hər hansı bir işçi stansiyasına yükləmək olar. Quraşdırılma prosesi başa çatdıqdan sonra "Administrative Tools" qovluğuna bir neçə yeni xidmət və "Active Directory Users and Computers" əlavə olunacaq. Lakin bir məqamı da yadda saxlamaq lazımdır ki, sözü gedən əlavə proqram vasitələri o zaman kompüterə və ya serverə yüklənə bilir ki, distributiv diskdə olan əməliyyat sisteminin dili kompüterdə işləyən əməliyyat sisteminin dili ilə eyni olsun. Yəni əgər korporativ şəbəkənin hər hansı bir işçi stansiyasında istifadə olunan əməliyyat sistemi MS Windows XP ingilis dilindədirsə, onda distributiv diskdə olan və server üçün nəzərdə tutulmuş əməliyyat sistemi də ingilis dilində olmalıdır. Belə olan halda bütün obyektlərin adı ingilis dilində olacaqdır.

4.4 Active Directory və onun funksiyaları

Windows platformasının mərkəzi komponenti olan kataloqlar xidməti "Microsoft Active Directory" – obyektlərin və şəbəkə mühitinin qarşılıqlı əlaqələrinin idarə olunması vasitələrini təqdim edir. "Active Directory" vasitəsi Microsoft Windows 2000 Server, Windows Server 2003 əməliyyat sistemini özək kimi qəbul edərək, onların əsasında idarəçiliyin keyfiyyətini yaxşılaşdırır, miqrasiya prosesini asanlaşdırır və proqram vasitələrinin işə salınması problemlərini həll edir. Əlavə olaraq "Active Directory" vasitəsi MS Windows Server 2003 əməliyyat sistemində şəbəkə kataloqlarını istifadə edən proqram təminatını yaratmaq üçün ən yaxşı seçimdir. "Active Directory" vasitəsinin inkişaf etdirilməsinin əsas məqsədi şəbəkəyə çəkilən ümumi

xərclərin azaldılmasıdır. Bu vasitənin bütün səviyyələrinin yaxşılaşdırılması və genişləndirilməsi ixtiyari arxitekturalı korporativ şəbəkələrin idarə edilməsi prosesinin universallaşdırılması, mühafizəliliyin artırılması və xərclərin azaldılmasına yönəlmişdir.

Active Directory vasitəsinin əsasları. Active Directory vasitəsi - MS Windows Server 2003 əməliyyat sistemləri ailəsi üçün kataloqlar xidmətidir (şəkil 4.13). Lakin Active Directory vasitəsinin MS Windows Server 2003 Web Edition versiyasında işləmək imkanı yoxdur, amma bu əməliyyat sistemi quraşdırılan kompüteri idarə etmək hüququ vardır. Active Directory vasitəsi obyektlər haqqında məlumatı şəbəkədə saxlayır, bu məlumatların axtarış və istifadəsi üçün rahat vasitələr təklif edir. İnformasiya kataloqlarının iyerarxik və məntiqi üslubda təşkil etmək üçün Active Directory vasitəsi struktur prinsiplərinə əsaslanan verilənlər bazasından istifadə edir.



Şəkil 4.13 Active Directory xidmətinin arxitekturası

Şəbəkə kataloqunun verilənlər bazası. Adətən şəbəkə kataloqunun verilənlər bazasını sadəcə "kataloq" (directory) adlandırırlar. Bu kataloq istifadəçilər, qruplar, kompüterlər, domenlər və təhlükəsizlik siyasətinin qaydaları kimi obyektlər haqqında məlumatı özündə cəmləşdirir. Bu məlumata giriş icazəsi ancaq korporativ şəbəkənin istifadəçilərinə və administratoruna verilə bilər. Kataloq özü fiziki olaraq domen kontrolleri kimi tanınan serverlərdə yerləşir, şəbəkə vasitələrinə və xidmətlər üçün əlçatandır. Domen bir neçə kontrollerə malik ola bilər. Hər bir kontrollerdə yerləşdiyi domen kataloqunun surətinin dəyişdirilmiş versiyası mövcuddur. Hər hansı bir kontrollerdə kataloqun dəyişdirilməsi domenin digər kontrollerlərinə və domenlər ağacına replikasiya olunur. Yazılmaq imkanı olan kataloqun replikasiyası və bütün kontrollerlərdə onun ehtiyat nüsxəsinin olması, korporativ şəbəkəyə məxsus istifadəçilərin və administratorların domendə kataloqa hər zaman stabil girişi əldə etməyə imkan verir. Kataloqun verilənləri "Ntds.dit" faylında domenin kontrollerində saxlanılır. Praktikadan məlum olduğu kimi bu faylı "NTFS" bölməli diskdə saxlamaq məqsədə uyğundur. Bəzi verilənlər kataloqun verilənlər bazası faylında saxlanılır. Digərləri isə, məsələn, qeydiyyat ssenariləri və ya qrup siyasətinin qaydaları, replikasiya olunan fayl sistemində yerləşir. Domen kontrollerləri arasında kataloqun verilənlərinin üç kateqoriyalı replikasiyası həyata keçirilir.

Domenin verilənləri. Bu domen daxilində yerləşən obyektlər haqqında məlumatdır. Adətən kataloqun informasiyası haqqında danışılanda məhz bu məlumatları nəzərdə tuturlar. Məsələn, elektron poçtların ünvanları, kompüter və istifadəçilərin atributları, şəbəkə resursları korporativ şəbəkənin istifadəçiləri və administratorları üçün maraq kəsb edən məlumatlardandır. Korporativ şəbəkədə yeni istifadəçi yaratdıqda domenin verilənlərində bu istifadəçinin qeydiyyat yazısının obyekti avtomatik olaraq öz əksini tapır. Təşkilatın kataloqunun obyektini

dəyişdirdikdə, yəni obyektin yaradılması, silinməsi və ya atributlarının yeniləri ilə əvəz olunması zamanı bu dəyişikliklər haqqında məlumat birbaşa domen verilənlərində yadda saxlanılır.

Konfiqurasiyanın verilənləri. Kataloqun topologiyası bütün domenlərin siyahısını və həmçinin, domenin kontrollerlərinin yerləşməsini və qlobal kataloqlarını özündə cəmləşdirir.

Sxemin verilənləri. Sxem - kataloqa yerləşdirilməsi mümükün olan bütün obyektlərin və atributların formal təyin olunmasıdır. MS Windows Server 2003 əməliyyat sistemi standart sxem təklif edərək bunun vasitəsi ilə sadalanan tipləri müəyyən edir: kompüterlərin və istifadəçilərin qeydiyyat yazıları, qrupları, domenləri və təhlükəsizlik siyasətinin qaydaları. Korporativ şəbəkənin administratorları və proqramçıları yeni tip obyektləri təyin edərək və ya mövcud obyektlərə yeni atributlar əlavə edərək bu sxemləri genişləndirə bilərlər. Sxemin obyektləri icazələrin idarə olunması siyahısı vasitəsi ilə (access control lists, ACL) mühafizə olunur. Bu da öz növbəsində ona təminat verir ki, sxemi ancaq icazəsi olan istifadəçilər dəyişdirə bilərlər.

4.5 Active Directory və təhlükəsizlik

Təhlükəsizlik elementləri, istifadəçinin sistemə daxil olan zaman autentifikasiya vasitəsi və kataloqların obyektlərinə girişlərinə nəzarət etmək Active Directory vasitəsinin daxili strukturunda nəzərə alınmışdır. Vahid qeydiyyat sistemi korporativ şəbəkənin administratoruna kataloqların verilənlərini və strukturunu ixtiyari nöqtədən idarə etmək imkanını verir. Müvafiq hüquqlu istifadəçilər isə icazə verilən ixtiyari resurslara giriş əldə edə bilərlər. Active Directory vasitəsi istifadəçilərin qeydiyyat yazılarının bazasını mühafizəli şəkildə və obyektlərə olan girişin hesabına, qruplar haqqında məlumatı özündə saxlayır. Active Directory vasitəsində yalnız istifadəçinin qeydiyyat verilənləri deyil, həmçinin, girişin idarə olunması məlumatları cəmlənir. Ona

görə də şəbəkədə qeydiyyatdan keçmiş istifadəçi avtomatik olaraq sistem resurslarına həm autentifikasiya, həm də girişin avtorizasiyası hüququna malik olur. Beləliklə, istifadəçinin korporativ şəbəkəyə daxil olduğu zaman təhlükəsizlik sistemi onu Active Directory vasitəsində saxlanan məlumatın köməyi ilə autentifikasiya edir. Əgər sonra istifadəçi şəbəkə xidmətinə giriş əldə etməyə cəhd göstərirsə, onda girişə diskresion nəzarət siyahısı (DACL - Discretionary Access Control List) bu istifadəçinin mühafizə olunan obyektə giriş imkanının olub-olmadığını yoxlamağa başlayır. Digər tərəfdən Active Directory vasitəsində istifadəçilər qrupunu yaratmaq mümkündür və bunun hesabına administratorlar üçün giriş hüquqlarını daha effektiv idarə etmək imkanı yaranır. Faylın xassələrini dəyişdirərək, onu qrupun bütün istifadəçiləri üçün oxunmağa açıq elan etmək olar. Belə olan halda Active Directory vasitəsinin obyektlərinə giriş qrupa olan üzvlük hüququ əsasında təyin olunur.

Active Directory sxemi – Active Directory vasitəsində yerləşdirilməsi mümkün olan obyektlərin görünüşünü və bu obyektlər haqqında olan məlumatın tipini müəyyən edən qaydalar yığımıdır. Bu qaydalar özü-özlüyündə adi obyektlərdir. Active Directory sxeminin obyektlərinin idarə edilməsi kataloqun digər obyektlərinin idarəçiliyindən qəti fərqlənmir. Active Directory sxeminin də iki tipini müəyyən etmək olar: 1) atributlar 2) siniflər. Atributlar və sinifləri aşağıdakı qaydada təsvir etmək olar:

Siniflər - kataloqun mümkün obyektlərini təsvir edirlər. Hər bir sinif atributlar toplusundan ibarətdir. Obyektin yaradılması zamanı atributlara obyekti təsvir edən məlumat yerləşdirilir. Məsələn, "User" sinfi "Network Address" (şəbəkə ünvanı), "Home Directory" (mənbə kataloqu) kimi atributlardan başqa daha bir neçə atributlardan ibarətdir. Active Directory vasitəsinin ixtiyari obyekti hər hansı bir obyektlər sinfinin nümayəndəsidir.

Atributlar siniflərdən ayrı təyin olunurlar. Hər bir atribut yalnız bir dəfə təyin olunur və bir neçə siniflərə aid olur. Məsələn, "Description" atributu, bir çox siniflər tərəfindən istifadə olunur, lakin sistemdə uyğunlaşmanı təmin etmək üçün bir dəfə təyin olunur. Atributlar obyektləri təsvir edirlər. Hər bir atributun öz şəxsi təsvir qaydası vardır ki, o da cari atribut üçün əvvəlcədən təyin edilən məlumatın tipini təsvir edir. Hər bir atributun sxemdə məlumatı təyin edən "AttributeSchema" sinfi ilə təsvir olunur. Belə təsvir olunma ixtiyarı atributun təsvir olunmasında iştirak etməlidir. Obyektə tətbiq olunan atributlar siyahısı obyektin məxsus olduğu sinif tərəfindən müəyyən olunur. Həmçinin, bu obyektin məxsus olduğu sinif bütün super-siniflərin tərəfindən müəyyən olunur. Atributlar dediyimiz kimi bir dəfə təyin olunurlar, lakin bir neçə dəfə istifadə oluna bilərlər. Belə yanaşma, cari atributu istifadə etməklə bütün siniflər arasında uyğunlaşma yaradır. Atributlar təkədədli və çoxədədli ola bilərlər. Atributa bir neçə qiymətin verilməsi bu atributun təyin olunma qaydasında göstərilir. Təkədədli atribut ya boş, ya da yalnız bir göstəriciyə malik ola bilər. Çoxədədli atribut isə boş və ya bir neçə göstəriciyə malik ola bilər. Çoxədədli atributun hər bir göstəricisi unikal olmalıdır.

İndeksləşdirilmiş atributlar. İndekslər atributlara tətbiq olunduğu kimi siniflərə tətbiq oluna bilmirlər. Atributların indeksləşdirilməsi verilmiş atributa malik obyektlərin tapılmasını tezləşdirmək məqsədi güdür. Əgər atribut indeksləşdirilmiş kimi nişanlanıbsa, indeksə yalnız bu atributun bütün elementləri deyil, müəyyən olunmuş sinfə münasibətləri də əlavə olunur. Yeni indeksləşdirilmiş atributların tətbiqi Active Directory vasitəsinin replikasiyası vaxtına, istifadə olunan yaddaşın və verilənlər bazasının ölçüsünə təsir göstərə bilər. Çünki verilənlər bazasının ölçüsü artmağa, replikasiya vaxtı isə uzanmağa başlayır. Çoxədədli atributlar da indeksləşdirilmiş ola bilərlər. Çoxədədli atributların indeksləşdirilməsi Active Directory vasitəsinin

ölçüsünün və obyektin yaradılmasına sərf olunan zamanın kəskin şəkildə artması ilə nəticələnir. Məhz bu səbəb təkədədli atributları çoxədədli atributlardan fərqləndirir. İndeksləşdirmək üçün atributları seçəndə onların həqiqətən də tez-tez istifadə olunacaqlarından və çəkilən əlavə xərclərin məhsuldarlıq ilə necə mütənasib olduğundan hökmən əmin olmaq lazımdır.

Sxemin indeksləşdirilmiş atributunun axtarışı Active Directory vasitəsinin verilənlər bazasından başqa, həmçinin cari atributun yerləşdiyi konteynerə əsasən aparıla bilər. Belə yanaşma axtarışı tezləşdirir və sistemin resurs ehtiyatlarından daha qənaətlə istifadə edir. Təcrübəli istehsalçılar və korporativ şəbəkənin administratorları yeni siniflər təyin etməklə və artıq mövcud siniflər üçün yeni atributlar müəyyən etməklə sxemi dinamik şəkildə genişləndirə bilərlər. Sxemin tərkib hissəsini domen kontrolleri idarə edir və sxem əməliyyatlarının sahibi (*schema operations master*) kimi çıxış edir. Sxemin ehtiyat nüsxələri domenin bütün kontrollerlərinə replikasiya olunurlar. Belə bir ümumi sxemin tətbiq olunması verilənlərin tamlığını təmin edir. Sxemi "Active Directory Schema" vasitəsi ilə də genişləndirmək mümkündür. Sxemin formasını dəyişdirmək üçün "Schema Administrators" qrupunun üzvü olmaq və "Active Directory Schema" vasitəsini sxem əməliyyatlarının baş kompüterinə quraşdırmaq lazımdır.

Sxemə hər hansı bir dəyişiklik etdikdə aşağıda sadalananları nəzərə almaq lazımdır.

- **Sxemin genişləndirilməsi qlobal xarakter daşıyır:** administrator sxemi genişləndirmək məqsədi ilə korporativ şəbəkənin lokal bir hissəsini genişləndirməlidir. Çünki sxemdə olan ixtiyari dəyişiklik korporativ şəbəkənin hər bir lokal hissəsinə aid olan domenin kontrollerlərinə replikasiya olunur;
- **Sxemin sistem sinifləri dəyişdirilə bilməz:** Active Directory sxemlərinin standart sistem siniflərini dəyişdirmək qadağandır, lakin sxemi dəyişdirən proqram vasitələri ilə qeyri-standart sistem

sinifləri əlavə etmək mümkündür. Məhz belə qeyri-standart sistem siniflərini administrator dəyişdirmək hüququna malikdir;

• **Sxemin genişləndirilməsi dəyişdirilə bilər:** siniflərin və ya atributların bəzi xassələri yaradıldıqdan sonra onu dəyişdirmək mümkündür. Sxemə əlavə olunmuş yeni sinif və ya atribut istənilən an dayandırıla bilər, lakin silinə bilinməz. Amma sistemin administratoru təyin olunmuş qaydaları nəzərə almamaq funksiyasını aktivləşdirərək, yenidən obyektlərin identifikatorunu istifadə edə bilər və ya siyahıda olan adlar vasitəsi ilə sxemin təyin olunmuş qaydalarını dəyişdirmək hüququna malik olar. Active Directory sxemin obyektlərinin pozulmasını dəstəkləmir. Lakin sistemdə obyektlər aktiv olmaya bilər və bu da təqribən obyektin silinməsi effektini verir.

Qlobal kataloq – Active Directory vasitəsinin bütün obyektlərinin ehtiyat nüsxələri saxlanılan domen kontrolleridir. Qlobal kataloq hər bir obyektin o atributlarını saxlayır ki, onlardan axtarış zamanı çox istifadə olunsun. Qlobal kataloq yerləşdiyi domenin və hissə şəklində də olsa digər domenlərin bütün obyektlərinin tam ehtiyat nüsxəsini özündə saxlayır. Belə yanaşma isə heç bir əlavə domen kontrollerinə müraciət etmədən effektiv axtarış aparmağı təmin edir. Qlobal kataloq avtomatik olaraq domenin ilk kontrollerində yaranır. Korporativ şəbəkənin administratoru qlobal kataloqu domenin digər kontrollerlərində işə sala bilər və ya onu domenin digər kontrollerinə keçirə bilər. Qlobal kataloqun rolu şəkil 4.14-də illüstrativ formada göstərilmişdir.

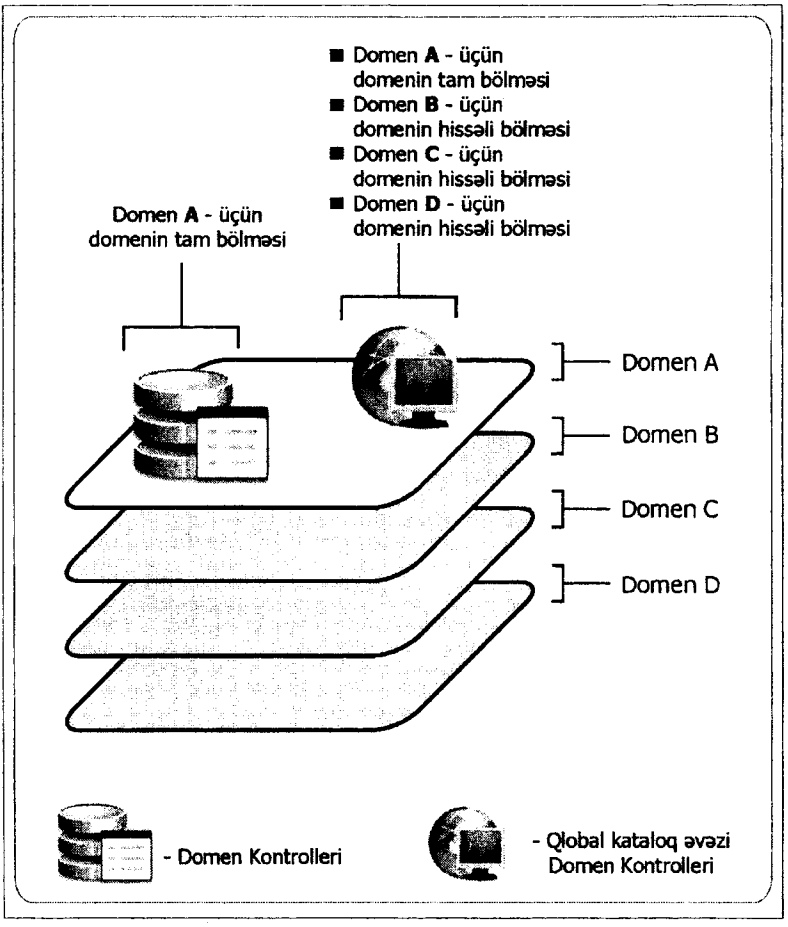
Qlobal kataloq aşağıdakı funksiyaları yerinə yetirir:

• **Qlobal kataloqun obyektlərinin axtarışı** Active Directory vasitəsinin bütün domenlərində informasiyanın yerləşmə məkanından asılı olmayaraq informasiya axtarışını təmin edir. Şəbəkədə bu tip axtarış çox böyük sürətlə və çox az şəbəkə trafiki istifadə edərək həyata keçirilir. Adətən korporativ şəbəkədə

printer və ya istifadəçi axtaranda, məsələn, "Start" menyusundan və ya sorğuda "Entire Directory" bəndini qeyd etdikdə, axtarış məhz qlobal kataloqda aparılır. Daxil edilmiş axtarış sorğusu qlobal kataloqun standart portuna yönəlir və sorğu emal olunmaq üçün qlobal kataloqa göndərilir.

• **Qlobal kataloqun istifadəçilərinin identifikatorlarının autentifikasiyası** qeydiyyat yazıları olmayan istifadəçiyə aid olan domen kontrollerlərində auutentifikasiyanın həyata keçirilməsi, istifadəçilərin identifikatorlarının axtarışına xidmət edir. Məsələn, əgər qeydiyyat yazısı "rahimov.com" ünvanında yerləşibsə və istifadəçi sistemə profilinə uyğun olaraq "elshan@rahimov.com" adı ilə "elshan2@rahimov.com" domenində yerləşən kompüterdən girməyə çalışırsa, "elshan2@rahimov.com" domen kontrolleri qeydiyyat yazısını tapa bilməyəcək və istifadəçi qlobal kataloqun serverinə giriş prosesini bitirmək üçün sistemdə lazımi addımları həyata keçirə bilməyəcək.

• **Çoxdomenli mühitdə universal qruplara üzvlük haqqında məlumatın dəstəklənməsi.** Qlobal qruplarda üzvlük haqqında məlumatdan fərqli olaraq, universal qruplarda üzvlük haqqında məlumat yalnız qlobal kataloqlarda saxlanılır. Məsələn, universal qrupun üzvü MS Windows 2000 Server əməliyyat sisteminin standart funksional səviyyəsində olan və ya daha yüksək səviyyəli domenə daxil olanda qlobal kataloq universal qruplara olan üzvlük haqqında məlumatı təqdim edir. Qlobal kataloq MS Windows Server 2003 əməliyyat sistemi çalışan sistemin domeninə daxil olduqda bu domen əlçatan deyilsə belə və əgər bu istifadəçi daha öncə sistemə heç olmasa bir dəfə daxil olubsa, kompüter dərhal formasını dəyişmiş məlumatı özündə qeyd edəcək. İstifadəçi bu domenə heç vaxt daxil olmamışsa, onda o yalnız lokal kompüterə daxil ola bilər. Lakin "Domain Administrators" qrupunun üzvləri korporativ şəbəkəyə qlobal kataloq əlçatan olmayanda da daxil ola bilərlər.



Şəkil 4.14 Qlobal kataloqun rolu

Active Directory xidmətində məlumatlar axtarışı. Active Directory xidmətinin əsas istiqamətlərindən biri də kataloqda olan istifadəçi və ya proqram tərəfindən müəyyən edilən obyektlərin axtarış sorğularının emal olunması üçün nəzərdə tutulmuşdur. Korporativ şəbəkənin administratorları və istifadəçiləri kataloqda məlumatları "Start" menyusunda olan "Find" komandasının köməyi ilə axtarıb tapa bilərlər. İstifadəçi kompüterində olan proqram vasitələri Active Directory xidmətinə "Active Directory

Services Interface" (ADSI) vasitəsinin köməyi ilə giriş əldə edə bilərlər. Active Directory xidmətinin əsas üstünlüklərindən biri də şəbəkə obyektlərinə məxsus müxtəlif məlumatların saxlanılmasıdır. Active Directory xidmətinin daxilində istifadəçilər, kompüterlər, fayllar, printerlər və digər avadanlıqlar haqqında məlumatları yerləşdirmək mümkündür. Məlumatlara girişin idarə olunması, giriş hüquqları vasitəsi ilə tənzimlənir. Müxtəlif təyinatlı şəbəkə məsələlərini yerinə yetirdikdə digər istifadəçilərlə qarşılıqlı əlaqəyə girmək və ya başqa şəbəkə resurslarından istifadə etmək lazım gəlir. Bu zaman müvafiq adları və ya ünvanları axtarıb tapmaq labüddür. Bu məsələnin həlli üçün Active Directory xidməti əvəz olunmaz bir vasitədir, çünki o təşkilat üçün vahid bir ünvan kitabçası rolunu oynayır. Beləliklə korporativ şəbəkəyə daxil olan ixtiyari istifadəçini onun adı, soyadı və ya elektron ünvanı vasitəsi ilə tapmaq olar. Bu tip axtarış qlobal kataloq vasitəsi ilə optimallaşdırılır. "Active Directory Users And Computers" bəndində olan "Advanced Find" dialoq pəncərəsi, korporativ şəbəkənin administratoruna imkan verir ki, idarəetmə məsələlərini daha effektiv şəkildə həyata keçirsin və həmçinin, kataloqdan seçilən verilənlərin süzgəcdən keçirilməsini daha rahatlaşdırsın. Bundan başqa, korporativ şəbəkənin administratorları minimal şəbəkə resurslarından istifadə etməklə çox çevik şəkildə qruplara obyektləri əlavə edə bilərlər. Bu zaman ehtimal olunan qrup üzvlərinin axtarışı üçün şəbəkə adinistratoru müvafiq sorğuları tətbiq edir.

4.6 Active Directory xidmətinin replikasiyası

Kataloqun replikasiyası verilənlərə daimi giriş əldə etməyə, dayanıqlığın artmasına, sistem üzərinə düşən yükün resurslar arasında bərabər paylanmasına və sistemin məhsuldarlığının artmasına təminat verir. Active Directory xidməti çoxtərəfli (*multimaster*) replikasiyadan istifadə edir. Bu da öz növbəsində kataloqu yalnız ilk və yeganə domen kontrollerində deyil, bütün

başqa kontrollerlərdə də dəyişmək imkanı yaradır. Çoxtərəfli model olduqca qüvvətli dayanıqlılıq xassəsinə malikdir. Bu modelin üstün cəhəti ondan ibarətdir ki, əgər kontrollerlərdən biri işləmirsə, bu digər kontrollerlərin işləməsinə mane olmur. Domen kontrolleri aşağıda sadalanan məlumatları özündə saxlayır və replikasiya edir:

• **Sxem məlumatı**

Active Directory xidmətində yaradılması mümkün olan obyektləri və onların malik ola biləcəyi atributları təyin edir. Bu tip məlumat bütün domenlər üçün ümumi xarakter daşıyır. Sxem məlumatları domenin bütün kontrollerlərinə replikasiya olunur.

• **Konfiqurasiya məlumatı**

Şəbəkənin məntiqi strukturunu xarakterizə edir və domenin strukturu, replikasiyanın topologiyası kimi məlumatları özündə cəmləşdirir. Bu tip məlumat bütün domenlər üçün ümumi xarakter daşıyır. Bu məlumatlar domenin bütün kontrollerlərinə replikasiya olunurlar.

• **Domen məlumatı**

Domenin bütün obyektlərini xarakterizə edir. Bu verilənlər domen üçün spesifikdir və digər domenlərə paylanılmır. Domen daxilində məlumatın daha tez tapılması məqsədi ilə bütün obyektlərin və domenlərin xassələrinin altçoxluğu qlobal kataloqda saxlanılır. Domenin verilənləri bu domenin bütün kontrollerlərinə replikasiya olunurlar.

• **Proqramların məlumatı**

Kataloqun tətbiqi bölməsində yerləşmiş məlumat, ancaq replikasiya əməliyyatının qlobal miqyasda lazım olmadığı hallar üçün nəzərdə tutulub. Bu proqram vasitələri administrator tərəfindən təyin olunmuş domen kontrollerlərinə yönəldilə bilər. Bu isə öz növbəsində replikasiya zamanı əlavə trafikin işlənməsinin qarşısını almış olacaq. Adətən saytlar Active Directory xidmətinə məxsus replikasiya əməliyyatının effektivliyini artırır. Konfiqurasiyanın və sxemin məlumatları

bütün domenə replikasiya olunur. Domenin məlumatları domenə məxsus bütün kontrollerlərə və bir hissəsi isə qlobal kataloqa replikasiya olunur. Replikasiya əməliyyatının həcmini azaldaraq, administrator şəbəkəyə düşən yükü azaltmış olur. Domen kontrollerlərinin saytlarını və replikasiyanın idarəetməsini (*replication change control*) replikasiya əməliyyatını optimallaşdırmaq üçün istifadə edirlər:

- istifadə olunan bağlantıları müntəzəm qiymətləndirərək, Active Directory xidməti ən effektiv şəbəkə bağlantılarını seçir;
- dayanıqlığı təmin etmək üçün, Active Directory xidməti replikasiya əməliyyatı zamanı bir neçə marşrutun dəyişdirilməsindən istifadə edir;
- replikasiya əməliyyatına lazım olan əlavə xərcləri azaldır. Buna isə yalnız dəyişikliyə məruz qalan məlumatları replikasiya etməklə nail olunur.

Əgər korporativ şəbəkənin daxili strukturunda saytların təşkil olunması, domen kontrollerləri arasında məlumat mübadiləsi nəzərə alınmayıbsa, onda istifadəçilər arasında olan məlumat mübadiləsinin xaotik şəkildə reallaşacağını ehtimal etmək olar. Saytlar korporativ şəbəkənin effektivliyini artırırlar. Active Directory xidməti məlumatları saytların daxilində daha çox replikasiya edir, nəinki, saytların arasında olan mübadilədə. Domen kontrollerlərinin arasındakı əlaqənin parametrləri və Active Directory xidmətindən müvafiq məlumatlara daha çox ehtiyacı olanlar ilk növbədə replikasiya olunurlar. Digər saytlarda olan domen kontrollerləri Active Directory xidmətinin bütün dəyişikliklərini fasilələrlə alırlar. Administratorlar bu prosesi müntəzəm olaraq ona görə yerinə yetirmirlər ki, şəbəkə üzərinə düşən yük azalsın. Həmçinin, saytlararası replikasiya zamanı məlumatların sıxılması hesabına da şəbəkəyə düşən yük azaldılır. Yeniləşmənin effektivliyini artırmaq, ancaq kataloqa yeni məlumat daxil edildikdə və ya kataloqun tərkib hissəsi dəyişdirildikdə, məlumat mübadiləsini həyata keçirməklə nail

olmaq olar. Kataloqun dəyişikliklərini domenin digər kontrollerlərinə müntəzəm şəkildə yayılması korporativ şəbəkənin müəyyən hissəsinin yüklənməsi ilə nəticələnir.

Replikasiya əməliyyatını administrator tərəfindən "Active Directory Sites And Services" vasitəsi ilə verilən məlumat əsasında indarəetmə vasitəsi olan "Active Directory Knowledge Consistency Checker" ilə həm avtomatik, həm də mexaniki optimallaşdırmaq olar. "Active Directory Knowledge Consistency Checker" vasitəsi Active Directory replikasiya topologiyasının sazlanması və dəstəklənməsinə cavabdehdir. Xüsusəndə "Knowledge Consistency Checker" vasitəsi replikasiyanın nə zaman yerinə yetiriləcəyini, məlumat mübadiləsi aparılacaq serverlər toplusunu təyin edir.

4.7 Active Directory xidmətinin istifadəçiləri

Active Directory xidmətinin istifadəçiləri quraşdırılan zaman MS Windows 2000 Professional və ya MS Windows XP Professional əməliyyat sistemində olan bir çox imkanlar sayəsində onlar daha köhnə sayılan Windows 95/98/NT4 əməliyyat sistemilərində də işləməyə başlayırlar.

Saytların dəstəklənməsi zamanı şəbəkəyə işçi stansiyaya ən yaxın olan domenin kontrollerindən daxil olmaq mümkündür.

Active Directory Services Interface. "ADSI" ssenariləri tətbiq etməklə Active Directory xidmətini idarə etmək mümkündür. Burada proqramçılar üçün Active Directory xidmətinə standart "API" tətbiq etmək mümkün olur.

Distributed File System (DFS). Burada MS Windows 2000 Server əmliyyatlar sistemi və ya digər əməliyyat sistemi ilə çalışan serverlərlə işləmək mümkündür. Bu serverlərdə "Windows .NET DFS" fayl sisteminin ümumi kataloqları saxlanılır.

NTLM 2.0 versiyasının autentifikasiyası. Burada MS Windows NT Server 4.0 əməliyyat sisteminin

"Challenge/Response Authentication" vasitəsinin 2-ci versiyasının ən mükəmməl autentifikasiya alətlərini işə salmaq mümkündür.

Active Directory Windows Address Book (WAB) vasitəsinin xassələr səhifəsi. Burada obyektin xassələri səhifəsində istifadəçinin telefonu, ünvanı və s. kimi məlumatları dəyişmək mümkündür.

Active Directory xidmətinin idarə olunması. Active Directory xidmətinin həm proqram, həm də istifadəçi interfeysi korporativ şəbəkənin idarə edilməsinin və inteqrasiya imkanlarının effektivliyini yüksəltmək məqsədi ilə təkmilləşdirilmişdir. Bir sıra yeni vasitələrin Active Directory xidmətində yaranması administratorların idarəetmə imkanlarını genişləndirir və daha effektiv edir. Belə yeni imkanlara misal, "Microsoft Management Console" (MMC) idarəetmə konsolunda əmələ gələn yeni bəndləri və obyektlərin seçilməsi (*object picker*) bəndini göstərmək olar. MMC vasitəsinin genişlənməsinə imkan verən komponentlər, obyektlər yığımını idarə etməyə imkan verir. Məsələn, belə olan halda korporativ şəbəkənin administratorları aşağıda sadalananları həyata keçirə bilərlər:

• Bir neçə obyektin xassələrini eyni zamanda seçib və redaktə edə bilərlər;

• Gələcəkdə istifadə etmək üçün Active Directory vasitəsinə olan sorğuların nəticələrini XML formatında yadda saxlaya bilərlər;

• Seçim etmək üçün yeni komponent olan "object picker" vasitəsini istifadə etməklə obyektlərin tez bir şəkildə seçilməsini təmin edə bilərlər.

Bu komponentin yenidən işlənilməsi böyük həcmli kataloqda obyektlərin axtarışı funksiyasını daha rahat və effektiv edir. Bununla yanaşı daha çevik sorğuların həyata keçirilməsinə şərait yaradır. İstifadəçi interfeysinin bir çox məqamlarında bu komponentə rast gəlmək mümkündür və digər istehsalçılar üçün də əlçatandır.

4.8 Sistemin məhsuldarlığının artırılmasının əlavə vasitələri

Active Directory vasitəsi ilə birgə işləyərkən məhsuldarlığın artırılmasının əlavə vasitələri aşağıdakı sadalananları özündə cəmləşdirir.

ACL vasitəsinin redaktə olunması. Bu interfeysin təkmilləşdirilməsinin əsas səbəbi, iş zamanı rahatçılığın daha da yüksəldilməsindən ibarətdir. Həmçinin konkret obyektə təyin olunmuş girişin varislik hüququnu tam şəkildə idarə etmək üçün istifadə olunur.

Genişlənmənin yeni imkanları. Müstəqil bir istehsalçının proqram təminatında işləyən administrator, Active Directory vasitəsini öz sisteminə qoşaraq, bu vasitənin üstün imkanlarından, qrupa müxtəlif obyektlər sinfini əlavə olunmasından və korporativ şəbəkənin idarə edilməsindən istifadə edə bilər.

Obyektlər. LDAP (Lightweight Directory Access Protocol) protokolunu dəstəkləyən, digər kataloqlardan olan istifadəçilər. 2798 nömrəli spesifikasiyasına uyğun olan "inetOrgPerson" sinfini tətbiq edən, LDAP kataloqunda təyin olunmuş istifadəçilər, Active Directory vasitəsinin istifadəçi interfeysi vasitəsi ilə təyin olunurlar. Active Directory vasitəsinin istifadəçiləri ilə işləyən interfeys, "inetOrgPerson" vasitəsinin obyektləri ilə də işləməyə qadirdir. Belə olan halda ixtiyari istifadəçi və ya kompüter "inetOrgPerson" vasitəsi ilə maneəsiz işləyə bilər.

Pasport ineqrasiyası. Pasport-autentifikasiyası indi artıq "IIS 6.0" tərəfindən dəstəklənir, bu da öz növbəsində obyekt-istifadəçiləri, onların Pasport-identifikasiyasına təqdim etməyə imkan verir. "IIS 6.0" vasitəsi HTTP-sorğular üçün istifadəçilər tərəfindən Local Security Authority (LSA) vasitəsinin köməyi ilə giriş markeri quraşdırır. Pasport xidməti olan İnternet istifadəçiləri, bu xidməti resurslara giriş əldə etmək üçün istifadə edə bilərlər. Bu istifadəçilər öz qeydiyyat yazılarını istifadə etməklə Active Directory vasitəsində olduğu kimi reallaşırlar.

ADSI xidməti ilə Terminal Server-in birgə istifadəsi. Terminal Server xidmətinin istifadəçi xassələrini "Active Directory Services Interface" (ADSI) interfeysini tətbiq edərək ssenarilərin yerinə yetirilməsi vasitəsi ilə quraşdırılır. Burada istifadəçilərin xassələrini Active Directory interfeysi və ssenarilər vasitəsi ilə təyin etmək olar. Belə yanaşma ADSI interfeysinin köməyi ilə proqramlaşdırılan dəyişikliklərin reallaşdırılmasını asanlaşdırır.

Replikasiyanı monitorinq etmək və etibar münasibətləri üçün WMI xassələri. "Windows Management Instrumentation" (WMI) vasitəsinin sinifləri domen kontrollerləri arasında Active Directory məlumatlarının replikasiyasının uğurla həyata keçməsinin monitorinqini aparmağa imkan verir. Çünki MS Windows 2000 Professional və MS Windows XP Professional əməliyyat sistemlərinin bir çox komponentləri domelər arası etibarlı əlaqələrdən istifadə edirlər. Bu vasitənin etibarlı əlaqələrin düzgün işləməsinin yoxlanılması prosesində böyük rolu var. Beləliklə, WMI vasitəsi ilə replikasiya zamanı baş verən problemlər haqqında administratorlara və istifadəçilərə xəbərdarlıq göndərmək mümkün olur.

MSMQ göndəriş siyahısı. "Message Queuing" (MSMQ) vasitəsində məlumatların Active Directory xidmətində olan yollama siyahısına (*distribution lists*) salınmasının dəstəklənməsi funksiyası əlavə olunub. MSMQ vasitəsinin istifadəçiləri Active Directory xidmətində yerləşən yollama siyahısını asanlıqla idarə edə bilərlər.

4.9 Məhsuldarlıq və miqyaslılıq

MS Windows Server 2003 əməliyyat sistemində quraşdırılmış Active Directory vasitəsində olan replikasiya mexanizmlərində və verilənlərin sinxronlaşdırılmasında hiss edilə biləcək dərəcədə yeniliklər və dəyişikliklər olunmuşdur.

Filialların dəstəklənməsi – adətən çoxfiliallı təşkilatlarda korporativ şəbəkə məsafədə yerləşən bir neçə şəbəkələrdən ibarət olur. Korporativ şəbəkənin bir hissəsi olan və məsafədə yerləşən şəbəkələrin hər birinin özünə məxsus domen kontrollerləri olmalıdır və onların hökmən təşkilatın mərkəzi ofisi ilə hər hansı bir kanalla əlaqəsinin olması vacibdir.

Windows Server 2003 əməliyyat sistemində istifadəçinin məsafədən sistemə daxil olması prosesi yaxşılaşdırılıb. Məsələn, sistemə istifadəçi hər dəfə daxil olduqda qlobal kataloqun mərkəzi serverinə daxil olmaq lazım deyil. Belə olan halda təşkilatlar özlərinə məxsus qlobal kataloqun mərkəzi serverini məsafədə yerləşən ofislərində proqram səviyyəsində açmaq məcburiyyətində deyillər. Adətən köhnə sistemlərdə domen kontrollerləri serverin domen kontrollerlərində qeydiyyatı zamanı qlobal kataloqlara müraciət edirdi. Lakin müasir sistemlərdə domen kontrolleri sistemə saytdan və ya qlobal kataloqların xarici serverlərindən öncədən heç olmasa bir dəfə daxil olmuş istifadəçilər üçün qlobal kataloqun üzvlük haqqında məlumatını keşləşdirir. Belə olan halda, bu istifadəçilərə sistemə daxil olmaq hüququ verilir və bu vəziyyətdə domen kontrollerinin qlobal kataloqun serverinə müraciət etməsinə heç bir ehtiyac qalmır. Bu da öz növbəsində əlaqə kanalları vasitəsi ilə müraciətlərin sayının azalmasına səbəb olur. Bundan başqa, belə yanaşma sistemin etibarlılığını artırır və qlobal kataloq funksional vəziyyətdə olmadıqda belə, istifadəçilərin sistemə girişlərini tam şəkildə izləmək olur.

Aşağıda Active Directory vasitəsinin tətbiqi nəticəsində sistemin məhsuldarlığının yaxşılaşdırılması öz əksini tapmışdır.

Saytlar arasında replikasiya zamanı verilənlərin sıxılmasının dayandırılması. Müxtəlif saytlarda yerləşən domen kontrollerləri arasında replikasiya zamanı verilənlərin sıxılması funksiyasını söndürmək imkanı mövcuddur. Bu isə öz növbəsində

domen kontrollerlərində prosessorun yükünün azaldılması hesabına məhsuldarlığın artırılmasına gətirib çıxarır.

Klasterləşdirilmiş virtual serverlərin dəstəklənməsi. Bəzən klasterləşdirilmiş serverlər üçün kompüter obyekti əvvəlcədən təyin olunur. Active Directory vasitəsini və klasterləri dəstəkləyən proqram təminatları, öz sazlama parametrlərini standart obyektlə qarşılıqlı şəkildə bağlayırlar.

Paralel LDAP qoşulma. Şəbəkə istifadəçilərinin autentifikasiyası məqsədi ilə bir qoşulmada bir neçə "LDAP" qoşulmalarına icazə verilir. Bu imkanı əlavə edərək, istehsalçılar "LDAP" qoşulmalarının və Active Directory vasitəsinin autentifikasiya sorğularının məhsuldarlığını artırır.

Domen kontrollerlərində artıq yüklənmədən mühafizə. Bu vasitə domenə yeni daxil edilən və bir neçə üzvü olan Active Directory xidmətinin domeninin ilk kontrollerini artıq yüklənmədən azad edir. Əvvəlki əməliyyat sistemindən fərqli olaraq məsələn, MS Windows NT Server 4.0 əməliyyat sistemində, domen MS Windows 2000 Server və MS Windows Server 2003 əməliyyat sistemində quraşdırılmış həm istifadəçi, həm də server kompüterlərini özündə saxlayır. MS Windows 2000 Service Pack 2 (SP2) və ya MS Windows Server 2003 əməliyyat sisteminin ilkin kontrollerini yeniləşdirən zaman o, MS Windows NT Server 4.0 əməliyyat sisteminin domen kontrollerinin davranış qaydalarının emulyasiyası kimi sazlana bilər. MS Windows Server 2003 əməliyyat sisteminin domen üzvləri, domen kontrollerinin yeniləşməsini MS Windows NT Server 4.0 əməliyyat sisteminin domen kontrollerlərindən ayıra bilməyəcəklər. MS Windows 2000 Server SP2 və ya MS Windows Server 2003 əməliyyat sisteminin üzvlərini elə qaydada sazlamaq olar ki, MS Windows 2000 Server SP2/Server 2003 əməliyyat sisteminin domen kontrollerlərini yeniləşdirən zaman onlara MS Windows NT Server 4.0 əməliyyat sisteminin domen

kontrollerinin davranış qaydalarının emulyasiyası funksiyasını dayandırmaq haqqında bildiriş gəlsin.

Qlobal kataloqun replikasiyasının sazlanması. Qlobal kataloqlarla replikasiya olan MS Windows Server 2003 əməliyyat sisteminin domenlərində qlobal kataloqun sinxronlaşdırma vəziyyəti yadda saxlanılır. Bu da öz növbəsində "Partial Attribute Set" (PAS) vasitəsinin generasiyası nəticəsində əmələ gələn verilənlərin həcmini azaldır. Verilənlərin həcminin azalması yalnız əlavə olunmuş atributların göndərilməsi ilə bağlıdır. Nəticədə replikasiyaya sərf olunan trafikin həcminin azalmasını və daha effektiv PAS yeniləşmələrini əldə etmək mümkündür.

Qrup daxilində üzvlük replikasiyasının yaxşılaşdırılması. Domenlər toplusu MS Windows Server 2003 Forest Native Mode rejiminə keçəndə qruplarda üzvlük haqqında məlumatlar toplanmağa və ayrı-ayrı üzvlər üçün repılikasiyalanmağa başlayır. Belə olan halda replikasiya zamanı şəbəkəyə və prosessor üzərinə düşən artıq yük ortadan qalxmış olur. Həmçinin eyni zamanda yeniləşmələr vaxtı məlumatların itirilməsi ehtimalı tam şəkildə aradan götürülür.

Dinamik yazılar üçün fəaliyyət göstərmə zamanının təyin olunmasının (Time to Live, TTL) LDAP vasitəsində dəstəklənməsi. Active Directory xidmətində dinamik yazılar saxlanıla bilər. Bu dinamik yazılar üçün "TTL" qiyməti təyin olunur. İstifadəçi bu göstəriciləri dəyişə bilər və bununla yazının fəaliyyət göstərmə zamanını artıra bilər. İstehsalçılar artıq Active Directory xidmətinin daxilinə uzun müddət saxlanılması tələb olunmayan məlumatlar yerləşdirirlər. Bu məlumatlar "TTL" zamanının bitdiyi vaxt avtomatik olaraq pozulurlar.

64-bitlik proqramların açılmasının dəstəklənməsi. "Aplication Deployment Editor" (ADE) vasitəsində qrup siyasətinin yeni parametrləri 32-bitlik proqramların 64-bitlik istifadəçilər üçün quraşdırılmasına və idarə edilməsinə imkan

verir. Qrup siyasəti korporativ şəbəkənin 64-bitlik istifadəçilərinə yalnız müvafiq proqramların yazılmasına təminat verir.

4.10 Konfiqurasiyanın idarə olunması

MS Windows Server 2003 əməliyyat sistemi effektiv sazlanmanı və çox sayda saytlara, domenlərə malik korporativ şəbəkələrdə olan Active Directory xidmətinin imkanlarını genişləndirir. Yeni quraşdırılma xidməti olan "Configure Your Server", Active Directory xidmətinin quraşdırılma prosesinin asanlaşdırır və konkret server üzərinə düşən öhdəliklərin (rolların) yenidən təyin olunmasını təklif edir. Bu isə öz növbəsində administratorlara serverin ilkin və əsas parametrlərini standartlara uyğun sazlamağa imkan yaradır. Serverin quraşdırılması prosesində administratorlar, istifadəçilərə əməliyyat sisteminin əlavə komponentlərini quraşdırmağa icazə verə bilərlər. "Configure Your Server" quraşdırılma xidməti aşağıdakı imkanları yaradır:

- ilkin başlanğıc parametrlərdən istifadə edərək, korporativ şəbəkədə ilk serverin DHCP, DNS və Active Directory vasitələrinin avtomatik sazlanması;
- administratorlara korporativ şəbəkənin digər serverlərinin sazlanmasında yardımçı olmaq. Bu xidmət administratorlara serverlərdə, məsələn, fayl-serverdə, çap-serverində, veb-serverdə, məsafədən idarəetmə vasitələrində (RAS) və marşrutizatorlarda lazım olan parametrləri işarələməklə yardımçı olur.

Korporativ şəbəkənin administratorları, bu vasitəni sapmalardan sonra bərpa əməliyyatı prosesində, server konfiqurasiyasının bir neçə kompüterə replikasiyası zamanı, quraşdırılmanı bitirmək üçün, serverin üzərinə düşən öhdəlikləri sazlayarkən və ya ilkin server konfiqurasiya olunarkən istifadə edə bilərlər.

Active Directory xidmətinin idarə edilməsində bir sıra yeniliklər mövcuddur:

DNS zonalarının avtomatik yaradılması. MS Windows Server 2003 əməliyyat sistemində "Domain Name System" (DNS) serverləri və zonalar avtomatik olaraq həm yaradıla və həm də sazlana bilər. Onlar korporativ şəbəkədə yeni zonaların yerləşdirilməsi üçün yaradılır. Belə yanaşma ixtiyari DNS serverinin sazlanma prosesini sürətləndirir.

Saytarası replikasiyanın topologiyasının yaxşılaşdırılmış generatoru. "Inter-Site Topology Generator" (ISTG) vasitələri çox sayda saytlara malik olan domenin dəstəklənməsini artıq yeni və yaxşılaşdırılmış alqoritmin köməyi ilə həyata keçirir. Beləliklə, korporativ şəbəkəyə məxsus ISTG generatoru rolunu oynayan domenin bütün kontrollerləri öz aralarında saytarası replikasiya haqqında qarşılıqlı şəkildə anlaşmalıdırlar. Domenlər toplusu "MS Windows Server 2003 Forest Native Mode" rejiminə keçməmiş, burada yeni alqoritmlər tətbiq oluna bilməz. "ISTG" generatorunun yeni alqoritmləri qarşılıqlı əlaqədə olan domenlərarası replikasiyanın məhsuldarlığını artırır.

DNS serverinin parametrlərinin genişləndirilməsi. Bu vasitənin köməyi ilə DNS konfiqurasiyasında olan səhvlər və qeyri-dəqiqlikləri aradan qaldırmaq xeyli asanlaşır və Active Directory xidmətinin işləməsi üçün lazım olan DNS infrastrukturunu düzgün sazlamağa geniş imkan yaranır. Bu yeni vasitənin üstün cəhətlərindən biri - "Active Directory Installation Wizard" vasitəsi kataloqun yeniləşdirilməsi və lazım olan hissənin replikasiyası üçün mövcud domen kontrolleri ilə əlaqə yaradan zaman domenin daxilində domen kontrollerinin işinin davam etməsidir. Əgər bu "Active Directory Installation Wizard" vasitəsi DNS konfiqurasiyasında olan səhv və ya sadəcə domen kontrollerinin işləməməsi ucbatından domen kontrollerini tapmayıbsa, onda bu vasitə səhvin yaranma səbəbini analiz edir və ekrana bu haqda məlumat çıxararaq, həmçinin bu səhvin aradan qaldırılması üçün təkliflər irəli sürür. Korporativ şəbəkədə domen kontrollerini axtarıb tapmaq üçün o, hökmən DNS domen

kontrollerlərinin axtarış yazılarında (*domain controller locator*) qeydiyyatdan keçməlidir. "Active Directory Installation" xidməti DNS infrastrukturunun düzgünlüyünü yoxlayır. Bu yoxlanış yeni domen kontrollerinin öz yazılarını dinamik olaraq DNS serverində yeniləmək üçün həyata keçirilir. Əgər yoxlanış zamanı DNS konfiqurasiyasında hər hansı bir nasazlıq müəyyən olunursa, onda dərhal ekrana bu nasazlıq haqqında və onu aradan qaldırmaq üçün məlumatlar verilir.

Ehtiyat nüsxələrdən replikasiyanın quraşdırılması. Active Directory xidmətinin tam verilənlər bazasının replikasiya etməkdənsə, bu vasitə korporativ şəbəkənin administratoruna imkan verir ki, başlanğıc replikasiya mənbəyi əvəzinə mövcud domen kontrollerinin və ya qlobal kataloqun serverinin ehtiyat nüsxəsi yerləşən faylları təyin etsin. Ehtiyat nüsxəsi yerləşən faylları Active Directory xidmətini dəstəkləyən ixtiyari ehtiyat nüsxə hazırlayan proqram vasitəsi ilə yaratmaq olar. Bu ehtiyat fayllarını yeni yaradılan domen kontrollerlərinə keçirmək mümkündür.

• **Miqrasiya vasitələrinin genişləndirilməsi**

MS Windows Server 2003 əməliyyat sistemində olan "Active Directory Migration Tool" (ADMT) vasitəsi aşağıdakı imkanları təqdim edir:

* ***Parolların miqrasiyası.*** MS Windows NT Server 4.0 əməliyyat sisteminin domenlərindən MS Windows 2000/Server 2003 əməliyyat sisteminin domenlərinə parolların miqrasiyasını tam təmin edir.

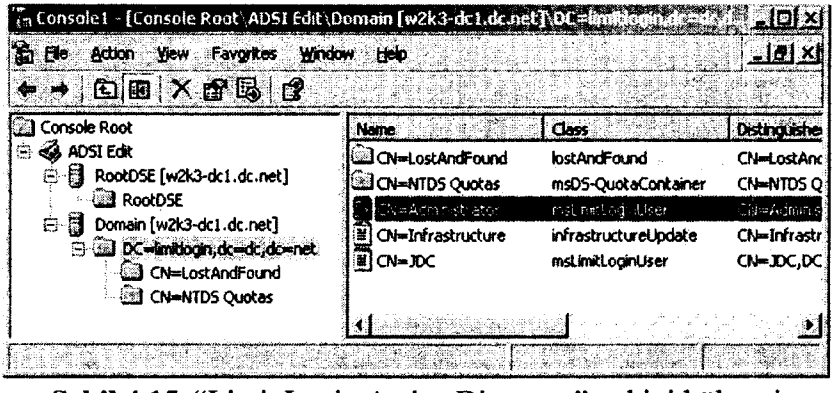
* ***Ssenarilər üçün yeni interfeys.*** İstifadəçilər, qruplar və kompüterlərin miqrasiyasını həyata keçirməyə imkan verir. Artıq ADMT vasitəsi COM-interfeysini dəstəkləyir və onu MS Visual Basic Scripting Edition, MS Visual Basic və MS Visual C++ kimi proqramlaşdırma dillərinin birində idarə etmək mümkündür.

* ***Komanda sətrinin dəstəklənməsi.*** Ssenarilər vasitəsi ilə həyata keçirilən bütün əməliyyatları korporativ şəbəkənin administratoru,

komanda sətrindən əmrləri daxil edərək reallaşdıra bilər.

* ***Təhlükəsizlik parametrlərinin yayımı.*** Təhlükəsizlik parametrlərinin yayımı, məsələn, "ACL" vasitəsində resursların təkrar tətbiq olunması yeni versiyalarda artıq elə qurulmuşdur ki, burada təhlükəsizliyin yayımı zamanı ilkin domen bütün hüquqlardan məhrum ola bilər (decommissioned). Artıq "ADMT" vasitəsi yayım üçün giriş məlumatı kimi istifadə olunan, yenidən quraşdırılma faylını təyin etməyə imkan verir. "ADMT" vasitəsinin yeni versiyası Active Directory xidmətinə keçidi sadələşdirərək prosesin avtomatlaşdırılması üçün yeni və effektiv imkanlar təqdim edir.

Tətbiqi bölmələr. Active Directory kataloqunun tətbiqi bölmələri adların kontekstinin və ya yeni tip bölmə olan tətbiqi bölmənin (*application partition*) yaradılmasını dəstəkləyir (şəkil 4.15). Təhlükəsizlik iştirakçılarından (*security principal*) başqa, adların konteksti ixtiyari tip obyektlərin iyerarxiyasını özündə saxlaya bilər. Onun üçün yalnız domen daxilində deyil, hətta domenin ixtiyari kontrollerinin replikasiyası sazlana bilər. Şəbəkənin işləməsinə heç bir xələl gətirmədən bu vasitənin köməyi ilə Active Directory xidmətində dinamik verilənləri yerləşdirmək olar.



Şəkil 4.15 "Limit Login Active Directory" tətbiqi bölməsi

Tətbiqi bölmələrdə inteqrasiyalaşdırılmış DNS zonalarının saxlanılması. DNS zonaları Active Directory xidmətinin tətbiqi bölmələri tərəfindən həm yadda saxlanıla bilər, həm də replikasiya oluna bilər. DNS verilənlərinin tətbiqi bölmədə saxlanılması qlobal kataloqda yerləşən obyektlərin sayını qoruyub saxlamağa imkan verir. Bundan başqa DNS zonasının verilənləri yalnız bu bölmə üçün ayrılmış domen kontrollerlərinə replikasiya olunurlar. Susma prinsipinə görə DNS üçün tətbiqi bölmələr yalnız DNS serverləri quraşdırılmış domen kontrollerlərini özlərində cəmləşdirirlər. Digər tərəfdən DNS zonasının tətbiqi bölmədə saxlanılması bu zonanı Active Directory xidmətinin digər domen kontrollerlərində quraşdırılmış DNS serverlərinə replikasiya etmək imkanını yaradır. DNS zonalarının tətbiqi bölmələrə inteqrasiyası informasiya replikasiyasının məhdudlaşdırmağa və şəbəkənin ötürmə qabiliyyətinə olan tələbləri azaltmağa imkan verir.

DirSync idarəetmə elementi. Active Directory xidmətində DirSync idarəetmə elementinin və kataloqda dəyişdirilmiş məlumatın seçilməsi olan LDAP elementinin dəstəklənməsi yeni versiyalarda daha da təkmilləşdirilmişdir. DirSync idarəetmə elementi standart LDAP axtarış zamanı baş verən yoxlanışlara analoji olaraq yoxlamalar həyata keçirə bilir.

Funksionallıq səviyyələri. Bu vasitənin köməyi ilə Active Directory xidmətinin özəyinin komponentləri hər bir domen kontrollerinə əlçatan olan imkanları təyin edə bilərlər. Belə yanaşma MS Windows 2000 Server əməliyyat sisteminin əsas domen prinsipində reallaşdırılmışdır. Bu mexanizm, həmçinin, MS Windows Server 2003 əməliyyat sistemində quraşdırılmış, lakin əvvəllər əməliyyat sisteminin daha öncəki versiyalarında çalışmış domen kontrollerlərinin işə salınmasının qarşısını almaq üçün istifadə olunur.

Siniflərin və sxemlərin atributlarının deaktivləşdirilməsi. Active Directory xidmətində olan yeniliklər Active Directory

siniflərinin və sxem atributlarının təyin edilməsini deaktivləşdirməyə imkan yaradır. Əgər ilkin təyin etmədə hər hansı bir səhv olarsa, onda siniflər və sxem atributları yenidən təyin oluna bilərlər. Deaktivləşdirmək funksiyası artıq təyin olunmuş və sistemdə çalışan sxemin atributunu və ya sinfini əvəz etmək imkanı yaradır. Bu hal adətən hər hansı bir xassənin parametrində səhv olduqda həyata keçirilir. Lakin bu əməliyyatı korporativ şəbəkənin administratoru istənilən zaman dayandırmaq hüququna malikdir.

Domenlərin adlarının dəyişdirilməsi. Bu vasitə artıq mövcud olan DNS və NetBIOS xidmətlərinin adlarını dəyişdirmək üçün nəzərdə tutulub. Həmçinin adın dəyişdirilməsindən sonra yeni domenin yüksək səviyyədə formalaşdırılacağına (*well formed*) təminat verir. Adı dəyişdirilmiş domenin identifikasiyası qlobal unikal identifikator (GUID) vasitəsi ilə həyata keçirilir, lakin domenin mühafizə identifikatoru (SID) dəyişilməz şəkildə qalır. Domenin adını dayişdirdikdə onun daxilində olan kompüterlərin üzvlük haqqı dəyişilməz qalır. Çünki bu vasitə ilə şəbəkənin əsas domenini dəyişdirmək mümkün deyil. Domenin adının dəyişdirilməsi prosesi domenin normal iş rejiminin dayandırılmasını və bütün domen kontrollerlərinin yenidən işə salınmasını tələb edir. Digər tərəfdən domenin adının dəyişdirilməsi prosesi domenin hər bir üzvünün öz sistemlərini iki dəfə yenidən işə salmasını tələb edir. Bu vasitə rəsmi qaydada domenin adının dəyişdirilməsi kimi idarəetmə sistemlərində tanınır və bu əməliyyatı müntəzəm həyata keçirilən tədbir hesab etmək düzgün olmaz.

Domen versiyasının yeniləşdirilməsi. Active Directory xidmətində olan növbəti üstünlüklərdən biri proqramların dəstəklənməsi və təhlükəsizliyə böyük yer ayrılmasıdır. MS Windows Server 2003 əməliyyat sistemi quraşdırılmış mövcud domendə birinci domen kontrollerini yeniləşdirmək üçün ilk növbədə bu yeniləşmə domenin texniki təlimatına uyğun

olaraq müvafiq qaydada işlənib hazırlanmalıdır. Domenin yeniləşdirilməsi üçün yeni sayılan sistem proqram "Adprep" mövcuddur. Adətən Active Directory vasitəsini MS Windows Server 2003 əməliyyat sistemi ilə çalışan serverlərə quraşdırdıqda "Adprep" sistem proqramının quraşdırılması tələb olunmur.

Replikasiyaların və etibar münasibətlərin monitorinqi. Korporativ şəbəkə administratorlarının domen kontrollerləri arasında məlumatların replikasiyasının uğurla başa çatmasını monitorinq etmək imkanları vardır. Çünki "MS Windows .NET Server" əməliyyat sisteminin komponentləri, məsələn, Active Directory xidmətinin replikasiyasını domenlərarası etibar münasibətlərində istifadə edirlər. Bu vasitə həmçinin domenlərarası etibar münasibətlərinin düzgün işləməsinin yoxlanılması metodunu təklif edir.

MS Windows Server 2003 əməliyyat sistemində WMI vasitəsi ilə Active Directory replikasiyalarının idarə olunması. Active Directory xidmətinin replikasiyasının monitorinqi çox sayda serverlərə və mürəkkəb topologiyaya malik korporativ şəbəkələr üçün xüsusən aktualdır. Bununla əlaqədar olaraq şəbəkə administratorları Active Directory xidmətinin replikasiyasını idarə etmək üçün müxtəlif instrumental vasitələrdən və istifadəçi interfeyslərindən (Replmon, Repadmin və "Microsoft Management Console" üçün olan "Active Directory Sites and Services" xidmətindən) istifadə etməlidirlər. "Microsoft Active Directory" (Common Information Model) vasitəsi "KCC" (Knowledge Consistency Checker) prosedurunun yerinə yetirilməsini təmin edir və Active Directory replikasiyası haqqında məlumat əldə etməyə imkan yaradır. "*root\MicrosoftActiveDirectory*" - adlar fəzasına və onların daxilində olan siniflərə baxmaq üçün "CIM Studio" vasitəsinin xidmətlərindən və ya "WQL" (WMI Query Language) sorğular dilindən istifadə etmək olar.

FƏSİL 5

KORPORATİV ŞƏBƏKƏLƏRDƏ İCAZƏLƏR SİYASƏTİNİN İDARƏ OLUNMASI

KORPORATİV ŞƏBƏKƏLƏRDƏ İCAZƏLƏR SİYASƏTİNİN İDARƏ OLUNMASI

- Korporativ şəbəkədə icazələr siyasətinin idarə olunması
- Korporativ şəbəkənin serverinə lokal giriş hüquqlarının məhdudlaşdırılması
- Konfiqurasiyanın idarə olunması
- Təhlükəsizlik şablonları
- İstifadə olunan proqramların məhdudlaşdırılma siyasəti
- InteliiMirror mexanizmində yeniliklər
- Korporativ şəbəkənin təhlükəsizlik və istifadəçi siyasətinin idarə olunması
- İstifadəçilərin miqrasiyası
- Korporativ şəbəkələrin məsafədən idarə olunmasının əsas elementləri

Fəsil 5. KORPORATİV ŞƏBƏKƏLƏRDƏ İCAZƏLƏR SİYASƏTİNİN İDARƏ OLUNMASI

Bu fəsildə korporativ şəbəkələrdə icazələr siyasətinin idarə olunmasının üstün cəhətləri ətraflı izah olunur. Belə yanaşma həm şəbəkə xidmətlərini, həm də istifadəçi resurslarının təhlükəsizliyini qorumağa imkan yaradır. Ümumiyyətlə ixtiyari korporativ şəbəkənin vahid bir idarəetmə siyasətinin olması və idarəetmə siyasətini MS Windows Server 2003 əməliyyat sistemi vasitəsi ilə həyata keçirmək üçün lazım olan addımlar geniş şəkildə şərh edilmişdir.

5.1 Şəbəkədə icazələr siyasətinin idarə olunması

İstifadəçinin qeydiyyat yazıları ilə birgə zəruri servislərlə şəbəkənin yaradılması, istifadəçiləri lazımi hüquqlarla təmin etmək və bu istifadəçilərin servislərdən istifadə etməyə imkan yaradılmasından başqa, bir sıra digər ə məliyyatları həyata keçirmək deməkdir. Korporativ şəbəkənin administratorunun işinin kifayət qədər böyük hissəsini icazələr siyasətinin idarə olunması təşkil etməlidir. İxtiyari korporativ şəbəkədə elə qovluq və fayllar mövcuddur ki, onlara şəbəkənin bütün istifadəçilərinin giriş hüququ olur, lakin elə resurslar da var ki, onlara yalnız məhdud sayda istifadəçilərin giriş hüququ nəzərdə tutulmuşdur. Korporativ şəbəkəyə məxsus çap qurğuları üçün düzgün təşkil olunmuş icazələr sistemi, istifadəçinin çap zamanı istədiyi şəbəkə çap qurğusunu seçməsi ilə işinin xeyli asanlaşdırması artıq praktikada özünü doğrultmuşdur və belə yanaşma beynəlxalq standartlarda da öz əksini tapmaqdadır.

Bəzən təşkilatın daxili strukturundakı şərait şəbəkə administratoru üçün əlverişli olmur. Belə vəziyyətdə bir-birinə zidd tələblər kimi problemlər ortaya çıxır məsələn, bir şöbədə olan istifadəçilərin bəzilərinin müəyyən fayllara və printerlərə giriş

hüququnun məhdudlaşdırılması. Müxtəlif obyektlərə giriş sisteminin təşkil olunması sxemi ayrı-ayrı təşkilatlarda müxtəlif tipdə ola bilər, lakin ümumi təməl prinsipləri eyni olması idarəetmə və təhlükəsizlik baxımından daha məqsədə uyğundur.

Bəzən şəbəkələrdə müxtəlif obyektlərə girişin qadağan olunması kifayət qədər formal və şərti xarakter daşıyır, lakin buna baxmayaraq bu korporativ şəbəkələrin iş prinsipini düzgün təşkil etməyə imkan verir. Baxdığımız fəsildə korporativ şəbəkəyə məxsus informasiyaya icazələr siyasətinin müxtəlif tələblərinin realizə olunması nümunələrinə nəzər yetiriləcək.

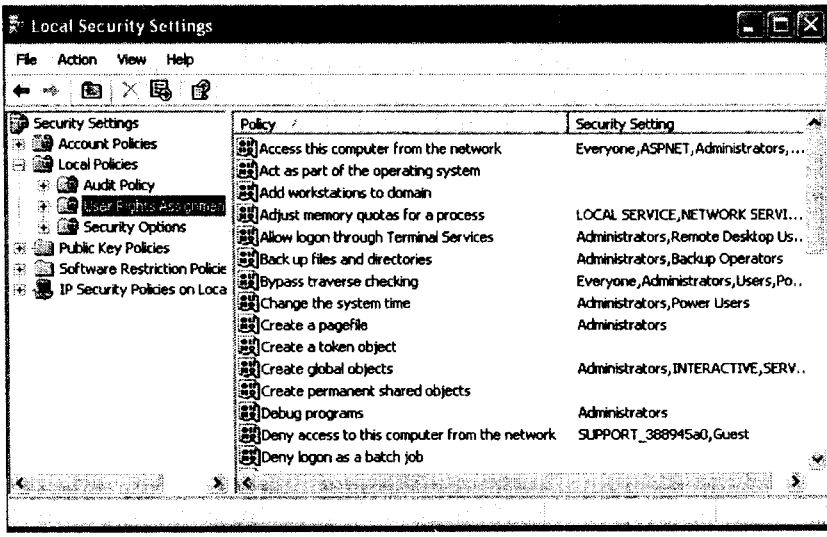
Korporativ şəbəkələrdə resurslara olan icazələrə müxtəlif yollarla nəzarət etmək olar. Məsələn fayl sistemi səviyyəsində hüquqları məhdudlaşdırmaqla və ya istifadə olunan proqramların işlənməsinə qoyulan qadağalarla. Bəzən bu qadağalar şərti olur. Əgər istifadəçi şəbəkə proqramlarından MS Access mühitində yazılmış hər hansı bir informasiyanı qəbul edirsə, onda proqram təminatına qoyulmuş bu məhdudiyyət prosesin başlamasına imkan verməyəcək. Adətən bu tip əlavə proqramlarda zəruri funksiyalara giriş parol vasitəsi ilə reallaşdırılır. Eyni zamanda istifadəçinin proqramı verilənlər bazasının özünə müraciət etdikdə, baza mühafizə olunmaması səbəbindən təhlükəli ola bilər. Lakin bacarıqlı istifadəçi bu təhlükəni öz xeyrinə həll edərək, bazadan istədiyi və özünə lazım olan informasiyanı əldə edə bilər. Bundan başqa o, verilənlər bazasının daxili strukturunu dəyişdirə bilər və bununla da verilənlərin tamlığını pozaraq, proqram təminatının düzgün işləməsinə mane olar. Verilənlərə girişin idarə olunmasının düzgün təşkil edilməsi zamanı qoyulan bütün qadağaların mümkün keçmə yollarını diqqətlə öyrənmək və test etmək lazımdır. Əgər belə bir keçid yolu varsa, onu həmin anda qapatmaq lazımdır. Dediklərimiz həcmcə çox böyük şəbəkələrə aiddir. Çox az istifadəçi sayına malik olan kiçik şəbəkələrin daxilində nadir hallarda bədəməl şəxs tapılar. Buna baxmayaraq sistemdə səhvlər və ya sapmalar ixtiyari zamanda baş verə bilər.

Bu aydın məsələdir ki, verilənlərin bazadan pozulması bərpa olunmasından dəfələrlə asan məsələdir. Giriş hüququ olan sadə istifadəçi tərəfindən verilənlərin bilmədən və heç bir bədniyyət olmadan pozulması verilənlər bazasının işinə ciddi ziyan vura bilər. Bu səbəbdən hər bir istifadəçi üçün giriş hüququ müəyyən etmək lazımdır, lakin bu iş həddindən artıq çətin başa gəldiyindən, bütün variantlarda verilənlərə olan icazələri qruplara ayırmaq məsləhətdir.

Şəbəkələrdə qrupların təşkilinin təməl prinsiplərinə görə giriş qruplarını şəbəkənin işçi stansiyalarından başlayaraq, şəbəkənin ən yüksəkdə duran strukturlarına qədər tətbiq etmək olar. Bizim baxdığımız halda ən yüksək struktur domendir. Qruplar ayrı-ayrı istifadəçilərdən və müxtəlif altqruplardan ibarət ola bilər. MS Windows XP əməliyyat sistemli işçi stansiyasını domenə qoşduqda, biz avtomatik olaraq domen administratorlar qrupunu kompüter administratorlar qrupuna daxil etmiş oluruq.
Qrupa fayl sistemləri və qrup siyasəti tərəfindən təyin olunan hüquqlar, bu qrupun bütün üzvlərinə şamil olunacaqdır. Müasir şəbəkə əməliyyat sistemi olan Windows ailəsinin ixtiyari versiyasında əvvəlcədən müəyyən olunmuş təhlükəsizlik şablonları mövcuddur ki, onların da təhlükəsizlik siyasətinin qurulmasında danılmaz rolları vardır. Əsas məqsəd isə təşkilati tələblərin yüksək səviyyədə yerinə yetirilməsindən ibarətdir.
Təhlükəsizlik şablonlarını mövcud təchizata əsasən müxtəlif variantlarda realizə etmək olar.

Təhlükəsizlik şablonları (Security Templates). Hazır təhlükəsizlik şablonlarını düzgün istismar etdikdə, onları şəbəkədə olan kompüterlərin təhlükəsizlik konfiqurasiyasının dəyişdirilməsi üçün də istifadə etmək mümkündür. Şəbəkə kompüterlərinin təhlükəsizlik konfiqurasiyasını komanda sətrindən işə salınan "Secedit.exe" köməkçi proqramının "Təhlükəsizliyin sazlanması və analizi" (Security Configuration and Analysis) təchizatı vasitəsi ilə və ya "Lokal təhlükəsizlik siyasəti" (Local Security

Policy) funksiyasına şablonu idxal etməklə dəyişdirmək olar. "Təhlükəsizlik parametrləri" (Security settings) komponentinə təhlükəsizlik şablonu yükləməklə, bir neçə kompüterin təhlükəsizlik konfiqurasiyasını dəyişmək mümkündür. Bu isə "Qrup siyasəti" (Group policy) funksiyasının genişlənməsi deməkdir. Təhlükəsizlik şablonları vasitəsi ilə həmçinin korporativ şəbəkənin zəif nöqtələrini və sistemin təhlükəsizlik siyasətinin pozulmasını "Təhlükəsizliyin analizi və sazlanması" təchizatının köməyi ilə müəyyən etmək mümkündür. Hələlik "Lokal təhlükəsizlik parametrləri" (Local Security Settings) təchizatını nəzərdən keçirək (şəkil 5.1). Bu təchizat MS Windows 2000 Server əməliyyat sistemindən başlayaraq bütün növbəti əməliyyat sistemlərinin versiyaları ilə çalışan kompüterlərdə realizə olunub. Bununla bərabər domen və domen kontrollerinin təhlükəsizlik siyasətinin elementlərini sazlamaq üçün bu təchizatda bir sıra parametrlər mövcuddur.



Şəkil 5.1 Lokal təhlükəsizlik parametrləri təchizatı

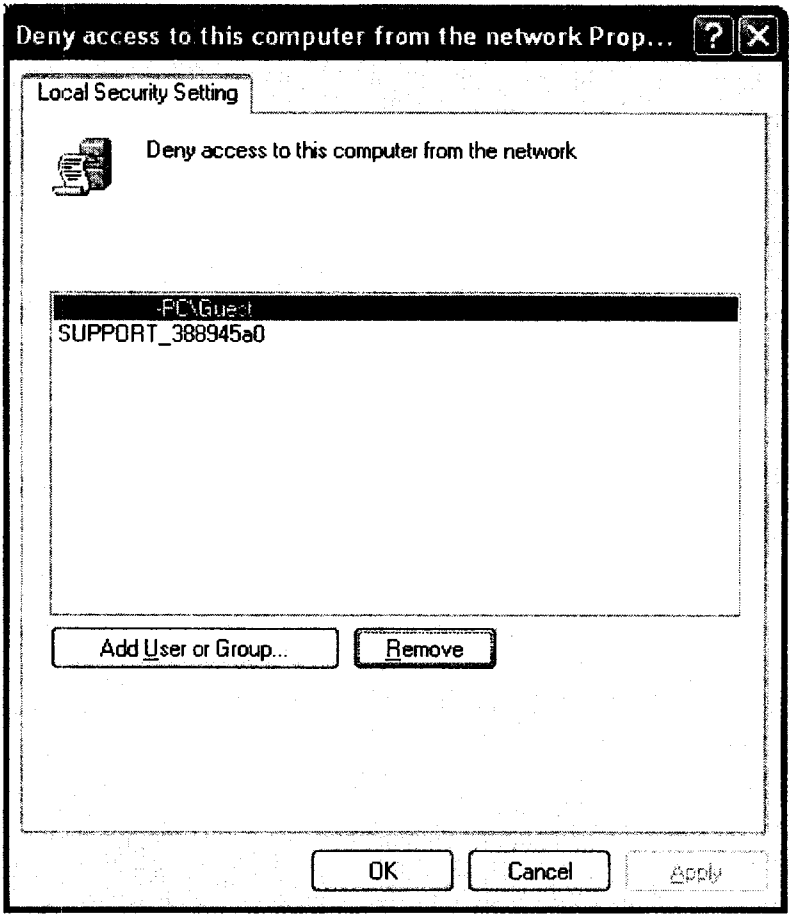
Adından məlum olduğu kimi təchizatlar, təhlükəsizlik siyasətini müxtəlif səviyyələrdə idarə etməyə imkan verir. Bu səviyyələr lokal domen kontrollerlərinə və domenlərə məxsusdur. Əgər bütün bu səviyyələrin hamısında təhlükəsizlik siyasəti mövcuddursa, onda ən yuxarıda olan səviyyənin siyasət qaydaları işləyəcək. Adətən bu səviyyələrin çoxunda heç bir təhlükəsizlik siyasəti təyin olunmur və bu səbəbdən ixtiyari səviyyədə təhlükəsizlik siyasətini tətbiq etmək olar. Lokal səviyyə, ən çox təhlükəsizlik siyasəti olan səviyyə sayılır. Onlar məhz server proqramlarının quraşdırıldığı kompüterin təhlükəsizliyini təmin edirlər. Domenin təhlükəsizlik siyasətini müəyyən etdikdə domen istifadəçilərinin təhlükəsizlik parametrlərini və hüquqlarını təyin etmək imkanı yaranır. Əslində bu o qədərdə vacib bir məsələ deyildir. Əsas olan isə onların hansı funksiyaları yerinə yetirdiyini bilmək və qarşıya qoyulmuş məqsədə çatmaq üçün uyğun gələn vasitələri seçməkdir.

5.2 Korporativ şəbəkənin serverinə lokal giriş hüquqlarının məhdudlaşdırılması

Əgər baxılan korporativ şəbəkə bir neçə təhlükəsizlik səviyyəsindən ibarətdirsə, bu o demək deyil ki, onlar bir-birindən asılı olmayan şəkildə təyin olunublar. Aydın məsələdir ki, serverin lokal sisteminə giriş əldə edib, bütün domenin işini qəsdən destruktiv və ya naşı şəkildə iflic vəziyyətə salmaq olar. Onda buradan belə bir nəticəyə gəlmək olar ki, istifadəçilərin serverə lokal girişinə tam qadağa qoymaq lazımdır.

Belə tip qadağanı realizə etmək üçün istifadəçilər qrupunu yaradaraq onlara "Lokal girişlərdən yayınma" (Deny logon locally) təhlükəsizlik siyasətini tətbiq etmək kifayətdir. Parametrlərin qiymətləri iki xanada əks olunur – lokal parametr və cari parametr. İkinci parametr göstəricisi mövcud təhlükəsizlik siyasətinin hansı səviyyədə tətbiq olunduğunu xarakterizə edir.

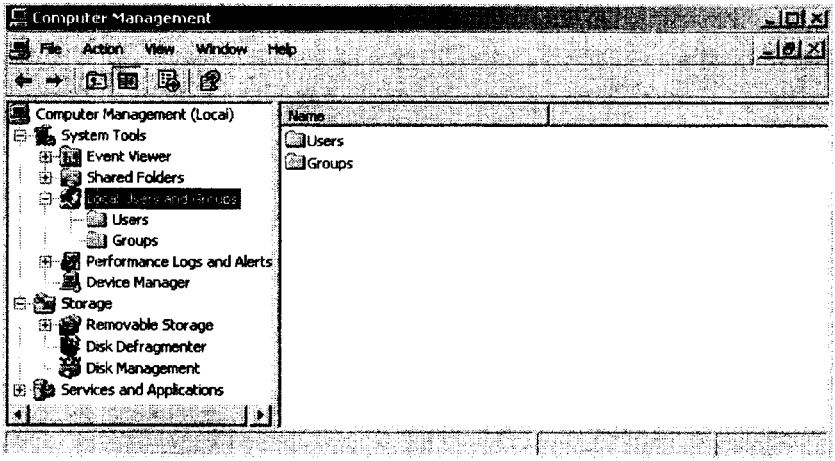
Şəkil 5.2-də göstərilmiş pəncərədə "Deny access to this computer from the network" şəbəkənin ixtiyari kompüterinə, habelə domen kontrolleri serverlərindən birinə olan girişin qabağını almaq olar.



Şəkil 5.2 Təhlükəsizlik parametrinin sazlanması

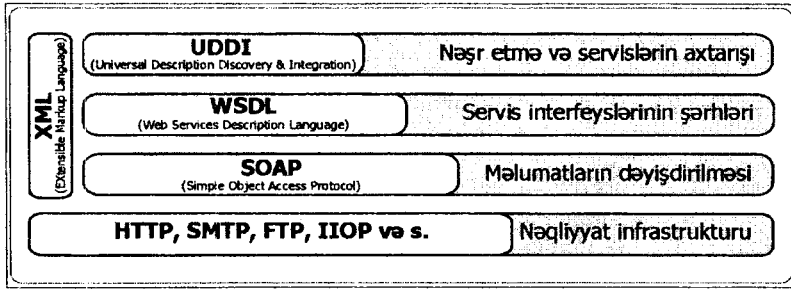
Bu qrupa daxil olunan istifadəçinin qeydiyyat yazıları və ya qruplar serverə lokal giriş imkanını itirmiş olacaq. Amma şəbəkə üzərindən girişə daha öncə icazə verilmişdirsə, onda o, olduğu

kimi qalacaq. Domen daxilində yaradılan qruplar öz istifadəçilərinin konkret hüquqlarını təyin etmək imkanına malikdirlər, lakin təyin olunmuş hüquqlar bir-birinə zidd olmamalıdırlar. Bu halda qrupların strukturunu təşkilatın tələblərinə uyğun müəyyənləşdirməyə imkan yaranır. Qrupların bir hissəsi avtomatik şəkildə yaradılır və yalnız məhdud sayda istifadəçilərə tətbiq oluna bilərlər. Kompüterdə olduğu kimi, domendə də ən yüksək hüquq statusuna domenin administratoru malikdir, sonra isə domenin digər üzvləri bu prioritet siyahısında yer alırlar. Lazım gəldikdə bunların sadəcə işlərini dayandırmaq olar. Yeni qruplar yaradaraq onları bir-birinin daxilinə və həmçinin sistem tərəfindən yaradılmış qruplara daxil etmək olar. Serverdə yalnız lokal qruplar, domenlərdə isə lokal və qlobal qruplar mövcuddur. Qrupların üzvlərinin hüquqları: bütün resurslara tam giriş hüququ və yaxud bəzi obyektlərə heç bir hüququnun olmamağı diapazonunda dəyişir. Bu diapazonun kənar qiymətlərinə real şəbəkə praktikasında administrator və qonaq (guest) hüquqlu istifadəçiləri göstərmək olar. Bir fakta nəzər yetirək, domen kontrollerinin serverində istifadəçilərin lokal qeydiyyat yazıları mövcud deyildir (şəkil 5.3). Müvafiq olaraq, domen kontrollerində fəaliyyət göstərən qeydiyyat yazılarının hər biri domendə müəyyən hüquqa malikdir. Buradan belə nəticəyə gəlmək mümkündür ki, əgər xaricdən əlçatan veb-servis və ya elektron poçt servisi təşkil etmək lazım gələrsə, bunu məhz bu iş üçün ayrılmış, hökmən ayrı bir serverdə etmək daha təhlükəsiz və idarəetmə baxımından daha məqsədə uyğundur. Bu adətən korporativ şəbəkələrdə ikinci server və ya servis serveri şəklində realizə olunur və bir sıra şəbəkə xidmətlərinin yerinə yetirilməsi funksiyasını daşıyır. Bədəmal şəxsin əlində olan proqram vasitələrinin mükəmməl olması ehtimalı yüksək olduğundan, onların ixtiyari şəbəkənin zəif nöqtələrindən istifadə edərək bir sıra xidmətləri ələ keçirmək ehtimalı da çox yüksəkdir.



Şəkil 5.3 Domen kontrollerində lokal qeydiyyat yazılarının olmaması

Domendə heç bir hüququ olmayan müstəqil şəbəkə kompüteri, yəni servis serveri bədəməl şəxs üçün şəbəkə resurslarının və servislərinin ələ keçirilməsini daha da çətinləşdirir. Eyni zamanda korporativ şəbəkənin veb-servis (şəkil 5.4) və ya elektron poçt servisindən müntəzəm istifadə edən istifadəçilərin də sistemə giriş imkanı olmamalıdır. Məlumdur ki, şəbəkənin təşkil olunmasının müxtəlif yolları mövcuddur, bu kitabda baxılan misallar sadəcə korporativ şəbəkənin yaradılması zamanı məhz hansı variantlardan istifadə etməyin daha məqsədəuyğun olduğunu müəyyənləşdirməyə yardımçı olacaq.



Şəkil 5.4 Veb-servislərin iyerarxik strukturu

5.3 İstifadəçi və altşəbəkələr

Elektron poçtun hüquqsuz istifadəçiləri poçt serverini sazlayan zaman ən çox rast gəlinən, poçt xidmətindən istifadə edən istifadəçilərin qeydiyyat yazılarının MS Windows əməliyyat sisteminin lokal qeydiyyat yazılarının avtorizasiya variantını nəzərdən keçirək. Bu halda hər bir poçt qutusunu yaratdığımız zaman, onun qeydiyyat yazıları müvafiq hüquqlarla avtomatik şəkildə formalaşır. Nəticə etibarı ilə bu istifadəçilərin hüquqları o qədər məhdudlaşdırılmışdır ki, onlar sistemə nə lokal, nə də korporativ şəbəkə vasitəsi ilə daxil ola bilirlər.

İkinci serverin "Kompüterin idarə edilməsi" (My computer / Manage) altmenyusunda istifadəçilərin xassələrinə baxdıqda, onların hamısının "POP3" qrupuna aid olduğu görünür. Lokal təhlükəsizlik siyasətinin xassələrində "Lokal girişlərdən yayınma" (Deny logon locally) funksiyasına rast gəlmək olar. "Şəbəkədən bu kompüterə olan girişə imtina" (Deny access to this computer from the network) bu qrup üçün təyin olunmamışdır. Halbuki, qrupun üzvlərinin öz poçt qutularına girişi zəruridir. Giriş yalnız poçt serveri vasitəsi ilə həyata keçirildiyinə görə bu qrup üçün qovluqlara (poçt qutularına) giriş nəzərdə tutulmamışdır. Adları qruplar siyahısında göstərilməyən bu tip serverin bütün istifadəçiləri bir sıra xüsusi qruplara avtomatik olaraq sistem tərəfindən daxil olunurlar. Bunlar əvvəlcədən quraşdırılmış qruplardırlar ki, onlarında əsas rolu fayl və qovluqlara tam hüququ olmayan istifadəçiləri tapıb müəyyən etməkdir.

Əgər avtomatik yaradılan istifadəçilərin hüquqlarını genişləndirmək lazım gəlmirsə, onda bu istifadəçilərin hüquqlarını dəyişdirmək tələb olunmur. Əgər belə məcburiyyət varsa, onda konkret istifadəçinin hüquqlarını dəyişdirmək məsləhət deyil, sadəcə onu artıq mövcud və ya yeni yaradacağınız qrupa yerləşdirmək kifayətdir və daha sonra bu qrupa müvafiq hüquqlar təyin etmək olar.

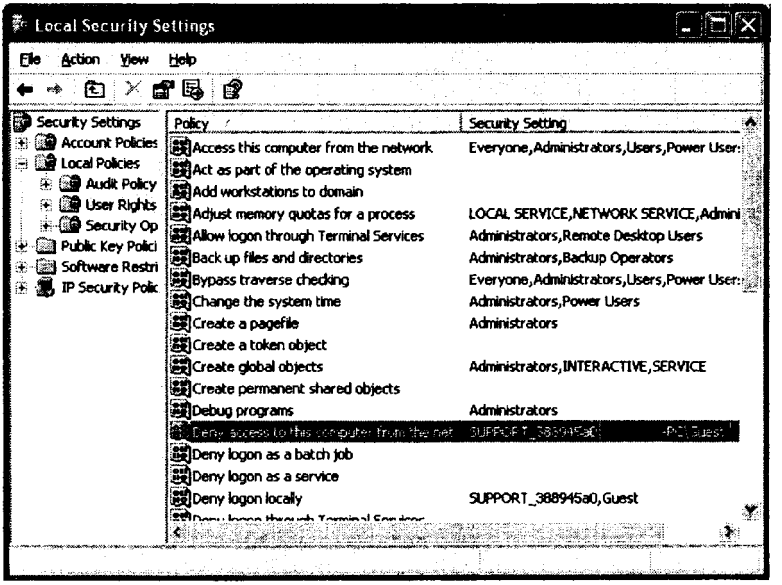
"İzolə edilmiş" altşəbəkələr. Bəzən praktikada elə hallara rast gəlmək mümkündür ki, korporativ şəbəkələrdə informasiya təhlükəsizliyinin qorunması məsələsi çox çətin həlli olan bir məsələyə çevrilir. Məsələn, təşkilatda administratorun qarşısına belə bir məsələ qoyulmuşdur: bir qrup istifadəçi (müdiriyyət) digər qrup istifadəçilərdən (işçilər) müəyyən informasiyanın son versiyasını çap olunmuş şəkildə qəbul etməlidir. Bu zaman birinci qrupun (müdiriyyət) ikinci qrupa (işçilər) aid kompüterlərində olan informasiyaya baxmaq icazəsi olmalıdır. Digər tərəfdən ikinci qrupun istifadəçilərinin, birinci qrupun kompüterlərinə giriş icazəsi olmamalıdır və onlara heç bir şəbəkə servisi vasitəsi ilə giriş əldə edə bilməməlidirlər. Belə bir məsələnin ən etibarlı həlli yollarından biri, domen tipli iki şəbəkənin qarşılıqlı şəkildə marşrutizator (*router*) vasitəsi ilə əlaqələndirilməsi və ortaq bir mühitin yaradılması təklifidir. Burada çap işini təşkil etmək üçün bütün istifadəçilərə əlçatan olan print-servislərindən istifadə etmək olar. Ancaq məsələni artıq qurğular almadan və ya artıq xərclər çəkmədən həll etmək lazımdır.

İlk baxışdan o qədər də mürəkkəb olmayan və adi korporativ şəbəkə çərçivəsində həll oluna biləcək bir məsləyə bənzəsə də, burada bütün tələbləri tam yerinə yetirmək o qədər də asan iş deyildir. Lakin informasiya təhlükəsizliyinin bəzi məqamlarını və bir neçə şəbəkə servislərinin istifadəsində olan narahatçılığı nəzərə almamaqla, həmçinin birinci qrup istifadəçiləri ikinci qrup istifadəçilərin domenindən çıxarmaqla, qarşıya qoyulan məsələ əlavə xərcsiz həll oluna bilər. Bu halda korporativ şəbəkənin əməliyyat gedən hissəsində kommunikasiyalar və fiziki struktur dəyişməz olaraq qalır, lakin məntiqi olaraq korporativ şəbəkənin əməliyyat gedən seqmenti iki hissəyə ayrılır.

Mövcud domendən çıxarılmış kompüterlər, hər hansı bir işçi qrupunun (*workgroup*) tərkibinə daxil olmalıdır. Bu işçi qrupun adı domenin adı ilə üst-üstə düşməməlidir. Bu kompüterlərin IP

ünvanları ehtiyatda sayılan ünvanlar diapazonundan ola bilər. Birinci qrupun işçi stansiyalarına qoşulan printerlərə icazəni əldə etmək üçün bu işçi stansiyalarda bir neçə dəyişikliklər etmək vacibdir. "Lokal təhlükəsizlik siyasəti" (Local Security Policy) bəndini açıb, "Lokal siyasətlər" (Local Policies) bəndində "Təhlükəsizlik parametrləri" (Security Settings) funksiyasını seçirik. Şəkil 5.5-də bu pəncərəni aydın şəkildə görmək olar. Açılmış pəncərədə aşağıda göstərilən üç parametri təyin etmək lazımdır:

- Şəbəkə girişi: lokal qeydiyyat yazılarının müştərək icazə və təhlükəsizlik modeli (Network access: Sharing and security model for local accounts).
- Şəbəkə girişi: SAM (Security Accounts Manager) qeydiyyat yazılarının sadalanmasına və ümumi resursların anonim istifadəçilər tərəfindən istifadəsinə icazə verilməməsi (Network access: Do not allow anonymous enumeration of SAM accounts and shares).



Şəkil 5.5 Lokal təhlükəsizlik parametrləri pəncərəsi

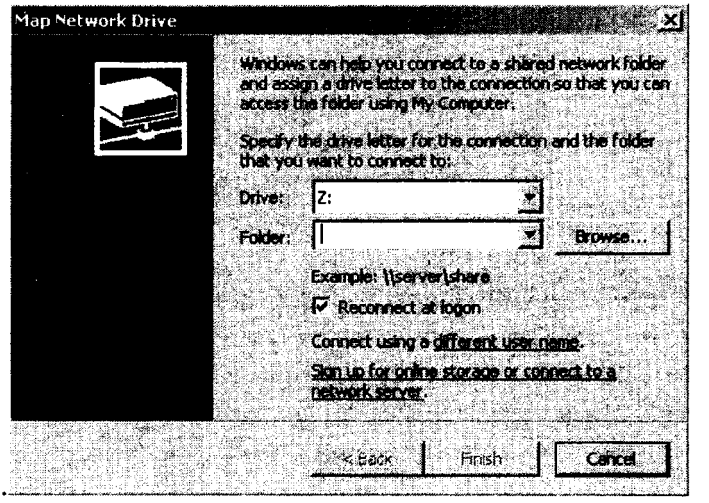
- Şəbəkə girişi: SAM (Security Accounts Manager) qeydiyyat yazılarının sadalanmasının anonim istifadəçilər tərəfindən istifadəsinə icazə verilməməsi (Network access: Do not allow anonymous enumeration of SAM accounts).

SAM (Security Accounts Manager) – mühafizəli verilənlər bazasında korporativ şəbəkənin istifadəçilərinin qeydiyyat yazıları saxlanılır. Bu parametrlərin birincisi üçün "Klassik" (Classic) qiymətini, digər ikisi üçün "Söndürülüb" (Off) qiymətini seçmək lazımdır.

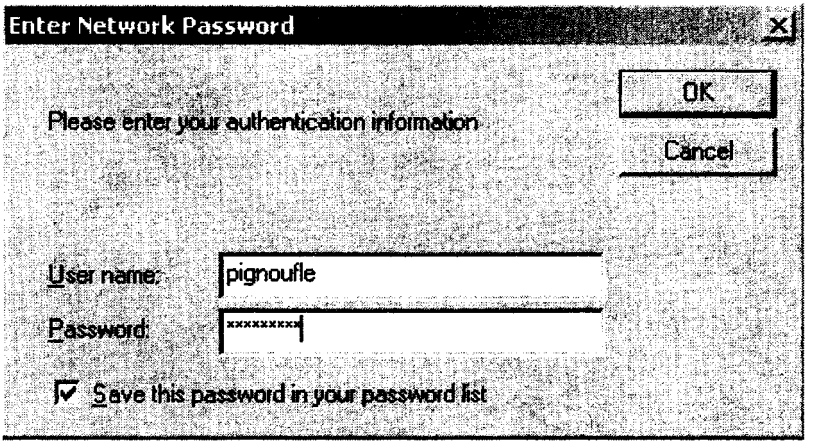
İzah olunan xassələr ancaq Windows XP Professional əməliyyat sistemi üçün yerinə yetirilə bilər. Əlavə olaraq birinci qrup istifadəçilərin kompüterlərində "Qonaq" (Guest) qeydiyyat yazısını aktivləşdirmək lazımdır. Ona boş parol və ümumi icazəli resursları təyin etmək məsləhətdir. Bunu etdikdən sonra artıq birinci qrupun kompüterləri şəbəkənin heç bir yerində gözə dəyməyəcək.

Birinci qrupun istifadəçilərinə qoşulmuş şəbəkə resursu və ya printer, korporativ şəbəkənin bütün istifadəçiləri üçün əlçatan olacaq. İkinci qrup istifadəçilərin resursları birinci qrup istifadəçilər üçün hökmən əlçatan olmalıdır. Bu məsələni reallaşdırmaq üçün istifadəçiləri domendə avtorizasiya etmək lazımdır. Ümumi resursları qoşmaq üçün kompüterləri əməliyyat sisteminə məxsus kompüter axtarış funksiyası və ya IP ünvan vasitəsi ilə müəyyən edib, standart funksiya olan şəbəkə diskini qoşub, kompüterin şəbəkədə olan adının yerinə IP ünvanını daxil edirik. Domenə daxil olan işçi stansiyalardan resursları qoşmaq üçün "Başqa adla qoşulma" (Connect using a different user name) funksiyasından isitfadə etmək lazımdır (şəkil 5.6). Bu funksiyanı seçərək, şəkil 5.7-də göstərilmiş pəncərə açılacaq və istifadəçinin adı və parolunu daxil etmək təklif olunacaq. Bütün tələb olunan resursları və printerləri qoşduqdan sonra, artıq tələb olunan rejimdə şəbəkənin işləməsinə nail oluruq. Daxili print-servislərə

malik printerləri qoşduqda, onların hansı qrupa aid olduqları və şəbəkənin hansı qovşağından qoşulduqları heç də önəm daşımır.



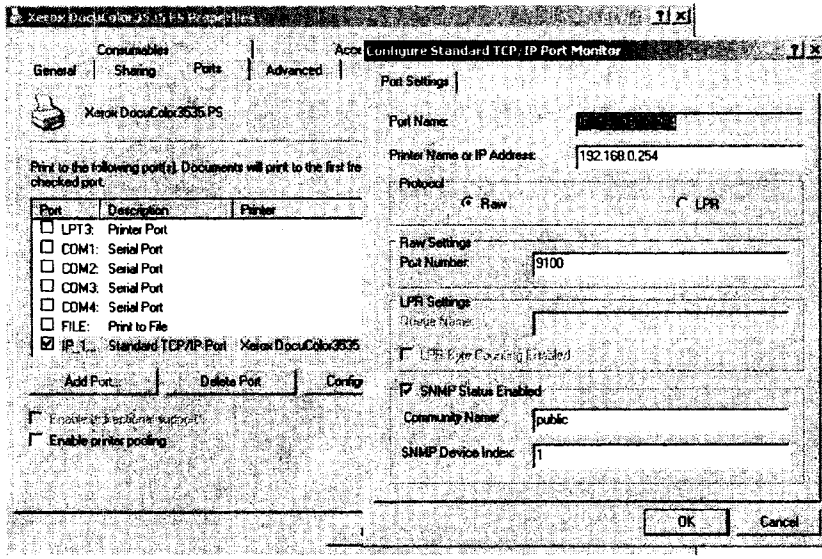
Şəkil 5.6 Şəbəkə resursunun qoşulması



Şəkil 5.7 Domen istifadəçisi adından şəbəkə resursunun qoşulması

Bu halda printerin özünə məxsus IP ünvanı vardır və hətta əgər onun bu ünvanı şəbəkənin IP ünvanına uyğun gəlmirsə, bu ünvan vasitəsi ilə ona qoşulmaq mümkündür. MS Windows XP əməliyyat sistemində printerləri qoşmaq üçün olan quraşdırılma servisi interaktiv rejimdə printerin portunu sazlamağa imkan verir. Bu məqsədlə şəbəkə printerinin lazım olan IP ünvanını və portunun tipini təyin edərək, əməliyyat sisteminin bu servisi olmadan da şəbəkə printerini şəbəkəyə daxil etmək olar.

Şəkil 5.8-də şəbəkə printeri portunun print-servis vasitəsi ilə mümkün quraşdırılma variantı göstərilmişdir. Müxtəlif istifadəçilərə məxsus print-servisli şəbəkə printerləri özünəməxsus xassələrə malikdir. Məhz bu səbəbdən belə qurğuları əldə edərkən, şəbəkə printerləri ilə bir dəstdə olan distributiv disklərini qoruyub saxlamaq məqsədə uyğundur. Bu disklərdə adətən funksionallığı ilə seçilən proqramlar yerləşdirilir ki, onlar da print-servislərin qoşulmasını və sazlanmasını, şəbəkədə IP ünvanların dəyişdirilməsi kimi işləri asanlaşdıra bilər.



Şəkil 5.8 Şəbəkə printerinin portunun sazlanması

İstifadədə, quraşdırılmada, idarəetmədə və platformaya uyğunlaşdırılmada daha sadə olan MS Windows Server 2003 əməliyyat sistemi, rahat mərkəzləşdirilmiş sazlama vasitələrini təklif edir. Bu vasitələrin köməyi ilə korporativ şəbəkədə olan silsilə xərclərin ümumi dəyərini də azaltmaq mümkündür. Şəbəkə idarəçiliyində olan digər üstünlüklərlə bərabər, mərkəzləşdirilmiş sazlama vasitələri MS Windows Server 2003 əməliyyat sisteminin şəbəkə administratorlarının işini xeyli yüngülləşdirir.

5.4 Konfiqurasiyanın idarə olunması

Adətən korporativ şəbəkənin istifadəçilərinə etibarlı iş mühiti tələb olunur və bu tələbi qarşılamaq üçün MS Windows Server 2003 əməliyyat sistemi tam uyğundur. MS Windows Server 2003 əməliyyat sistemini vasitəsi ilə dəyişiklikləri və konfiqurasiyanı idarə etmək, həmçinin çox rahat idarə oluna bilən infrastrukturun yaradılması mümkündür. Bu özəllik xüsusən böyük şirkətlərin korporativ şəbəkələrində bir neçə qrup istifadəçilərin eyni layihə üzərində çalışdığı zaman özünü doğruldur. Bu zaman məqsədə operativ və etibarlı şəkildə çatmaq həddindən artıq asanlaşır. Belə struktur adətən fərdi kompüterlərdən və ya işçi yerinə qoyulan terminallardan ibarət ənənəvi korporativ şəbəkənin üzərində yaradılır və paylanmış ofis adlanır.

Paylanmış ofis strukturunda istifadəçilərə unifikasiya olunmuş etibarlı mühit, düzgün sazlanmış əməliyyat sistemi, bütün şəbəkə proqramlarının yeni versiyaları və qoşulma nöqtəsindən asılı olmayaraq informasiya resurslarını birbaşa əldəetmə imkanı tələb olunur.

İnformasiya texnologiyaları şöbəsi təşkilatın korporativ şəbəkəsinin istifadəçilərinin tələblərini tam şəkildə yerinə yetirməlidir. Belə şəraitdə aşağıda sadalanan bir sıra faktorlara dərhal reaksiya göstərmək lazımdır:

- yeni əməliyyat sistemi və gündəlik istifadədə olan proqramları;
- əməliyyat sistemi və gündəlik istifadədə olunan proqramların müntəzəm yeniləşməsi;
- yeni avadanlıq;
- konfiqurasiyanın müntəzəm dəyişdirilməsi;
- biznesin yeni tələbləri;
- yeni istifadəçilər;
- korporativ şəbəkənin təhlükəsizlik problemləri.

Bu sadalanan dəyişikliklərə sonsuz bir proses kimi baxmaq olar (şəkil 5.9). İdarəetmə vasitələrini və konfiqurasiyasını sazlamaq üçün texniki vəsaitlərin daim əlçatan olması administratorun işinə böyük kömək kimi dəyərləndirilə bilər:

- aşağıda sadalananların ümumi dəyərinin minimallaşdırılması;

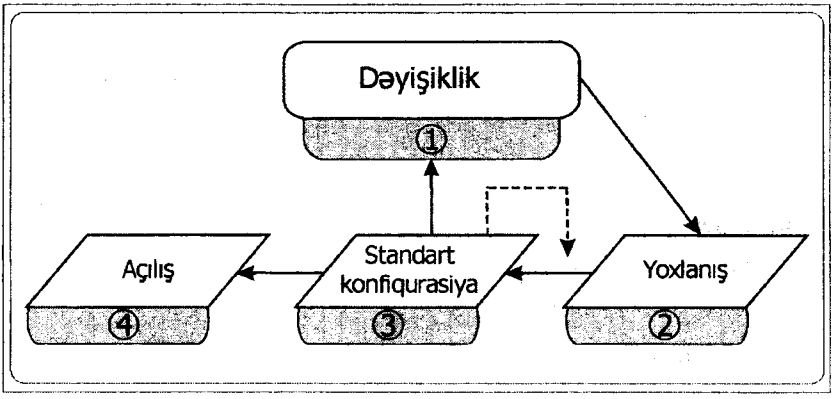
- sapmalardan sonra boş dayanma və bərpa zamanının minimuma endirilməsi;
- korporativ şəbəkəyə məxsus işçi stansiyalarda qeyri-effektiv quraşdırılma ilə əlaqədar əlavə işlərin minimuma endirilməsi;
- aparat təminatının sapmaları nəticəsində dayanmaların minimuma endirilməsi;

- iş qabiliyyətinin aşağıdakı vasitələr ilə artırılması;

- resurslara daimi girişin təmin olunması;
- proqramların məsafədən quraşdırılması və yeniləşdirilməsi;
- istifadəçilərin resurslarına, verilənlərinə və parametrlərinə girişi, onların şəbəkəyə qoşulma yerindən asılı olmayaraq, müstəqil şəkildə təmin olunması.

Qrup siyasəti tərəfindən təklif olunan "Software Installation" vasitəsi, proqram təminatı açılışının sadə sxemləri üçün nəzərdə tutulmuşdur. Korporativ şəbəkələrdə proqram vasitələrinin quraşdırılması zamanı cədvəl üzrə işin təşkili, inventarlaşdırma, hesabatlılıq və şəbəkə üzərindən quraşdırma funksiyaları tələb olunduqda "Microsoft Systems Management

Server 2.0" (SMS) proqram təminatından istifadə etmək məqsədə uyğundur.



Şəkil 5.9 Konfiqurasiya və dəyişiklikləri idarəetmə prosesi

5.5 Təhlükəsizlik şablonları

Təhlükəsizlik şablonları (security templates) korporativ şəbəkələrin təhlükəsizlik siyasətini müəyyən etməyə kömək edir. Digər tərəfdən təhlükəsizlik şablonları sistemin təhlükəsizliyinin bütün aspektlərini özündə cəmləşdirən vahid bir nöqtədir, yəni bu şablonlar heç bir yeni parametrlər daxil etmirlər, sadəcə bütün mövcud təhlükəsizlik altsistemlərini bir yerə cəmləyərək, şəbəkənin idarə edilməsini asanlaşdırırlar. Təhlükəsizlik şablonlarını qrup siyasətinin obyektinə (Group Policy Object - GPO) idxal edərək domenin idarəetmə işini asanlaşdırmış oluruq və domenin təhlükəszilik sistemini dərhal sazlamaq imkanı əldə edirik.

Təhlükəsizlik şablonları aşağıdakı parametrləri həyata keçirməyə imkan verir:

- qeydiyyat yazılarının siyasətini;
- parolların siyasətini;
- qeydiyyat yazılarının kilidlənməsi siyasətini;
- Kerberos siyasətini;

• lokal siyasətini;
• audit siyasətini;
• istifadəçilərin hüquqlarının idarə olunmasını;
• təhlükəsizlik parametrlərini;
• sistem jurnalların parametrləri: *Application, System və Security;*
• məhdud imkanlı qrupları; təhlükəsizlik baxımından vacib sayılan qruplarda üzvlüyü;
• sistem servislərinin işə salınması və giriş hüquqlarının parametrlərini;
• reyestrin bölmələrinə giriş hüququnu;
• qovluq və kataloqlara giriş hüququnu.

Təhlükəsizlik şablonları **.inf** faylı şəklində sistemdə yerləşirlər. Bu isə öz növbəsində şablonların bəzi atributlarını əldə etmək, idxal və ixrac etməyi asanlıqla həyata keçirməyə şərait yaradır. IP Security (IPSec) və açıq açarlar siyasətindən başqa, bütün atributlar bir təhlükəsizlik şablonunun daxilində yadda saxlana bilərlər.

Windows Server 2003/XP əməliyyat sistemlərində standart şablonlar mövcuddur, onlar müxtəlif səviyyəli təhlükəsizliyi təmin edir və aşağıdakı məqsədlər üçün nəzərdə tutulur:
• parametrlərin təkrar sazlanması;
• yüksək mühafizəlilik səviyyəsi olan mühitin realizə olunması;
• mühafizəliliyi tam yüksək səviyyədə olmayan, lakin tam uyğun gələn mühitin yaradılması;
• sistemin kökünün qorunması.

Burada yeni təhlükəsizlik şablonu yaratmaq və ya standart şablonlardan istifadə etmək mümkündür. Məsələn, "Setup security.inf " təhlükəsizlik şablonu təhlükəsizlik parametrlərini ixtiyari variantda sazlamağa imkan verir. Odur ki, o əməliyyat sistemi kompüterə yüklənilən zaman aktivləşir və lokal şəkildə istifadə olunur. Təhlükəsizlik parametrlərini dəyişməzdən öncə, yeni təyin edəcəyiniz parametrlərin praktikada özünü necə doğruldacağını yoxlamaq zəruridir.

5.6 İstifadə olunan proqramların məhdudlaşdırılma siyasəti

İnternet texnologiyalarının və elektron ünvan sistemlərinin geniş yayıldığı bir zamanda müxtəlif təyinatlı proqramların istifadəçi kompüterlərinə yol tapması çeşidli variantlarda baş verir. Belə halda istifadəçilər tanış olmayan proqramların işə salınması haqqında qərar verməli olurlar. Troyan proqram tipli olan viruslar müntəzəm olaraq özlərini digər proqramlar kimi sistemə tanıdıb və istifadəçiyə təqdim edirlər ki, onları istifadəçi işə salsın. Proqram təminatının istifadəsini məhdudlaşdıran siyasət (software restriction policies) kompüteri və ya şəbəkəni icazəsi olmayan və ya etibarlı olmayan proqram təminatlarının işə salınmasından qoruyur. Qrup siyasətinin obyektləri (Group Policy Objects - GPO) üçün təhlükəsizlik səviyyəsini təyin etmək mümkündür, məsələn: məhdudiyyətsiz (unrestricted) və ya qadağan olunmuş (disallowed), bu da öz növbəsində icazəli/icazəsiz proqramların işə salınmasını avtomatlaşdırılmasına gətirib çıxarır. Digər tərəfdən konkret proqram təminatları üçün standart təhlükəsizlik səviyyəsini dəyişmək mümkündür. Məsələn, əgər ilkin olaraq proqram təminatının təhlükəsizlik səviyyəsinə "qadağan olunsun" qaydası qoyulubsa, onu dəyişərək yeni qaydalar təyin etmək mümkündür. Proqram təminatının istifadəsini məhdudlaşdıran siyasət, qrup siyasətinin obyektləri üçün təyin olunmuş təhlükəsizlik səviyyələrini və qaydalarını özündə cəmləşdirir. Bu siyasəti korporativ şəbəkənin domeninə, lokal şəbəkələrə və ayrı-ayrı kompüterlərə tətbiq etmək olar. Proqram təminatının istifadəsini məhdudlaşdıran siyasət, proqramları müxtəlif üsullarla identifikasiya etmək qabiliyyətinə və həmçinin, infrastrukturun ümumi siyasətinə uyğun olaraq bu və ya digər proqram təminatının işə salınıb və ya salınmamağı haqqında qərar vermək imkanlarına malikdir.

İstifadəçilər isə funksional-inzibati qaydalara uyğun olaraq korporativ şəbəkənin administratorları tərəfindən təyin olunan bütün bu qaydalara riayət etmək məcburiyyətindədirlər.

Proqram təminatının istifadəsini məhdudlaşdıran siyasət, aşağıdakı imkanları yaradır:

• korporativ şəbəkənin hər hansı bir işçi stansiyasında ixtiyari proqramın işə salınmasının idarə olunması, məsələn, elektron ünvandan gələn viruslardan qorunmaq üçün, elektron poçt sisteminin qovluqlarından bir sıra proqram fayllarının işə salınmasına məhdudiyyət qoyulması;

• çoxistifadəçili işçi stansiyasında, yalnız əvvəlcədən müəyyən olunmuş konkret faylların və ancaq lazım olan proqramların işə salınmasına icazə verilməsi;

• işçi stansiyasına hansı istifadəçinin etibarlı proqram təminatı istehsalçıları (trusted publishers) siyahısını artırmaq hüququna malik olduğunu təyin etməyə imkan verməsi;

• proqram təminatının istifadəsini məhdudlaşdıran siyasətin korporativ şəbəkənin bütün işçi stansiyalarına şamil olub, olmadığını təyin etməyə imkan verməsi;

• lokal işçi stansiyada seçilmiş ixtiyari faylların domendə işə salınmasının qadağan edilməsi, sırf viruslu fayların domenin digər istifadəçilərinin kompüterlərinə keçməsinin qarşısını almaq məqsədi ilə tətbiq olunması.

İxtiyari növ korporativ şəbəkədə proqram təminatının istifadəsini məhdudlaşdıran siyasətin antivirus proqram vasitələrinin yerinə işlədilməsi tam yanlış və effektsizdir.

Windows Update. Bütün dünyada milyonlarla istifadəçilər hər həftə Windows Update funksiyasının köməyi ilə Windows əməliyyat sisteminin yeniləşmiş versiyasını (update) öz kompüterlərinə yazırlar. Windows Update – müvafiq sayta daxil olandan sonra, kompüterin əməliyyat sisteminin hansı versiyasına malik olduğunu təyin edərək, ona lazım olan kritik yenilikləri təklif edir. Bu halda baxmayaraq ki, yeniləşmə İnternet üzərindən aparılır, amma əməliyyat sistemin təhlükəsizliyi və mühafizəliliyi tam şəkildə qorunur. Windows Update proqramı istifadəçilərin tam rahatlığını təmin etmək üçün özü müntəzəm şəkildə kritik

(Critical Update Notification) və avtomatik yenilikləri (Automatic Updates) təklif edir.

Auto Update – bu funksiya vasitəsi ilə administratorlar təhlükəsizlik elementlərini, sistemdə olan ciddi səhvləri, yeni qurğunun drayverlərini yeniləşdirmək imkanına malikdirlər. "Auto Update" funksiyası sistem administratorlarına kritik yeniləşmələrin və bir neçə kompüterin yenidən işə salınmasında əvəzsiz yardım edir. Düzgün sazlanma zamanı əgər "Auto Update" daxili korporativ servislərin yeniləşmələri ilə uyğun gəlirsə, onda kompüterdə mümkün olan bütün yeniləşmələrə ciddi şəkildə nəzarət edə bilər. Avtomatik yeniləşmə funksiyası əməliyyat sistemi daxilində həm avtomatik, həm də administrator tərəfindən təyin edilmiş zamanlarda yerinə yetirilə bilər.

Dynamic Update – sistemin kompüterə yazıldığı zaman mövcud olan çatışmazlığını aradan qaldırmaq üçün istifadə olunur. Məsələn, əməliyyat sisteminin diskində olmayan yeni drayverlərin yazılması üçün istifadə oluna bilər.

Qurğların drayverləri – Windows Server 2003 əməliyyat sistemi administratorlara kömək olaraq, istifadəçilərə veb saytdan yeni sertifikatlaşdırılmış drayverlərin yüklənməsi imkanını yaradır. Digər tərəfdən "Plug and Play" servisi və qurğuların dispetçeri ilə inteqrasiyanı təmin edir.

Proqram təminatının yeniləşmə servisi – Software Update Services. Müasir biznes aləmində şirkətlər korporativ şəbəkə istifadəçilərinin xaricdən müvafiq qaydalara uyğun olaraq yoxlanılmamış yeniləşmələri qəbul etmələrinin heç də tərəfdarı deyillər. Bu vəziyyətdən çıxış yolu kimi, Microsoft korporasiyası tərəfindən korporativ mühafizə vasitələrindən birinin quraşdırılmasını göstərmək olar. Microsoft Software Update Services (SUS – proqram təminatının yeniləşmə xidməti) – Windows 2000/Server 2003 əməliyyat sistemi olan daxili serverlərə İnternet vasitəsi ilə Windows Update rəsmi saytında çıxan bütün kritik yeniləşmələrini lazımı vaxtda yüklənməsi və

quraşdırılması xidmətini təqdim edir. Burada sistemi elə sazlamaq olar ki, administrator rəsmi saytda çıxan kritik yeniləşmə haqqında məlumatları öz elektron ünvanına mütəmadi olaraq, xəbərdarlıq şəklində alsın. Hal-hazırda Windows 2000 Server əməliyyat sisteminin genişlənməsi (add-on) kimi təklif olunan "SUS" xidməti, administratorlara korporativ şəbəkənin serverlərində, Windows 2000 Professional / XP Professional əməliyyat sistemli işçi stansiyalarında kritik yenilikləri dərhal reallaşdırmağa imkan verir.

Proqram təminatının yeniləşmə xidməti (S US) aşağıdakı özəllikləri təklif edir:

• **Microsoft Software Update Services** – server komponenti olub Windows 2000 Server/Server 2003 əməliyyat sistemi olan kompüterlərə yazılır. Windows Update saytı ilə sinxronlaşaraq Windows 2000/XP əməliyyat sistemi üçün olan bütün kritik yeniləşmələri əldə edir. Sayt ilə sinxronlaşma həm avtomatik, həm də sistem administratoru tərəfindən reallaşdırıla bilər. Yüklənmiş yeniləşmələri bir-bir sınaqdan çıxarıb, hansının daha uyğun olmasına qərar vermək olar.

• **Avtomatik yeniləşmənin istifadəçiyə aid hissəsi** – bu komponent korporativ şəbəkənin Windows 2000 Profcssional/XP Professional əməliyyat sistemi olan işçi stansiyalarında və Windows Server 2003 əməliyyat sistemi ilə çalışan serverlərə quraşdırılmaq üçün nəzərdə tutulub. Bu xidmətin köməyi ilə korporativ şəbəkənin serverləri və işçi stansiyaları proqram təminatının yeniləşmə xidməti (SUS) quraşdırılmış xüsusi serverə qoşularaq, lazım olan yeniləşmələri yükləmək imkanına malikdirlər. Burada işçi stansiyanın hansı yeniləşmə serverinə qoşulması bir dəfə müəyyən edilir və buna uyğun cədvəl tərtib olunduqdan sonra, prosesin avtomatlaşdırılması mümkün olur. Bu prosesi Active Directory və ya qrup siyasəti vasitələri ilə həyata keçirmək olar.

• **Mərhələli açılma** – bu prosesi həyata keçirmək üçün SUS – proqram təminatının yeniləşmə xidməti yeniləşməni korporativ şəbəkənin bir neçə serverinə yükləyir. Bu serverlərin biri ehtiyat serveri ola bilər və bunun funksiyası ilkin yeniləşmələri sınaqdan çıxarmaqdan ibarətdir. Əgər bu sınaq serverində yeniləşmə uğurla həyata keçirsə, onda bu yeniləşməni artıq korporativ şəbəkənin bütün işçi stansiyaları və serverlərinə yönəltmək olar. Bu yolla korporativ şəbəkənin işçi stansiyalarının və serverlərinin əməliyyat sisteminin sıradan çıxmayacağına təminat vermək olar.

• **Serverarası sinxronlaşma** – korporativ şəbəkənin serverlərinə və işçi stansiyalarına yeniləşmə serverinin maksimum yaxın yerləşdirilməsini təmin etmək üçün bir neçə proqram təminatının yeniləşmə xidməti (SUS) serveri lazım ola bilər. Bu halda SUS xidməti, Windows Update saytının yerinə başqa SUS xidməti göstərən serverin ünvanını göstərməyə imkan verir, bu da öz növbəsində korporativ şəbəkə daxilində kritik yeniləşmələrin rahat bir şəkildə yayılmasına imkan yaradır. SUS xidmətinin əsas məqsədi MS Windows 2000/XP/Server 2003 əməliyyat sistemlərinin kritik yeniləşmələrini korporativ şəbəkəyə daha tez çatdırılmasıdır. Praktikadan məlum olduğu kimi bir sıra şirkətlər öz təhlükəsizliyini qorumaq məqsədi ilə proqramların yayılmasında elektron vasitələrdən istifadə edirlər, məsələn, Systems Management Server (SMS). Bu sistemin köməyi ilə proqram vasitələrini tam idarə etmək, təhlükəsizliklə və viruslarla mübarizədə bir sıra problemləri köklü şəkildə həll etmək mümkündür.

5.7 InteliiMirror mexanizmində yeniliklər

"IntelliMirror" idarəetmə mexanizmləri – konfiqurasiya və dəyişiklikləri idarə etmək üçün çox qüvvətli bir vasitədir. IntelliMirror idarəetmə mexanizmi özündə məhsuldarlığın mərkəzləşdirilməsi və paylanmış hesablamaların çevikliyi keyfiyyətlərini cəmləşdirir. Bu çevik mexanizm istifadəçinin

parametrlərini, verilənlərini və proqramlarını korporativ şəbəkənin bir nöqtəsindən digər nöqtəsinə keçirdikdə tam əlçatan olmasına təminat verir. Artıq yeni nöqtədən istifadəçi korporativ şəbəkəyə qoşulduqda bu parametrlər olduğu kimi qalırlar. Bundan əlavə, korporativ şəbəkənin administratoru, əməliyyat sistemini uzaqdan sazlamaq üçün məsafədən quraşdırılma vasitələrini (Remote Installation Services – RIS) tətbiq edə bilərlər. IntelliMirror vasitəsinin bir çox alətləri qrup siyasətini istifadə edirlər. Belə yanaşmada isə Active Directory xidmətinin istifadəsi qaçılmazdır. Microsoft Windows 2000 Server/Server 2003 əməliyyat sistemlərində Active Directory xidməti tam dəstəklənir. IntelliMirror vasitəsinin MS Windows XP/Server 2003 əməliyyat sistemlərində dəstəklənən bir çox alətləri, MS Windows 2000 Server əməliyyat sistemində də dəstəklənir.

IntelliMirror vasitəsini, sadalanan əməliyyat sistemlərinin biri və ya bir neçəsi işləyən korporativ şəbəkədə tətbiq etmək olar. Lakin MS Windows XP/Server 2003 əməliyyat sistemlərində olan yeniliklər və əlavələr idarəetməni və qeydiyyat yazılarını daha çevik və rahat şəkildə həyata keçirməyə təminat verir. İnformasiyanın intellektual idarə edilməsinin parametrlərinin və proqramlarının xassələrinə əsasən, IntelliMirror vasitələri istifadəçi verilənlərinin şəxsi parametrlərinin və ümumiyyətlə, hesablama mühitinin əlyetənlik səviyyəsini artırır. Əvvəlcədən təyin olunmuş siyasət qaydalarına əsasən IntelliMirror vasitələri istifadəçi verilənlərinin, proqramlarının və MS Windows 2000/Server 2003 əməliyyat sistemində işləyən mühitlərin şəxsi parametrlərinin açılmasını, bərpa edilməsini və dəyişdirilməsini təmin edir. Faktiki olaraq IntelliMirror vasitəsi istifadəçi üçün onun şəxsi hesablama mühitinin izlənməsi funksiyasını yerinə yetirir. Belə halda, istifadəçilər korporativ şəbəkənin hansı nöqtəsindən və hansı bağlantı növü ilə sistemə qoşulmaqlarından asılı olmayaraq, özlərinə məxsus informasiyaya və proqram təminatına dərhal giriş əldə edə bilirlər. IntelliMirror vasitəsi

korporativ şəbəkənin administratoruna bir dəfə proqram təminatının istifadəsi qaydalarını təyin etməklə, artıq gələcəkdə onun heç bir müdaxiləsi olmadan bu qaydaların korporativ şəbəkənin bütün işçi stansiyalarına avtomatik şəkildə tətbiq olunacağına təminat verir. IntelliMirror vasitəsinin özəyini aşağıdakı vasitələr təşkil edir:

• **Siyasətin idarə olunası.** Qrup siyasətinin parametrlərini düzgün təyin etdikdən sonra korporativ şəbəkənin bütün kompüterlərinə və istifadəçilərinə şamil etmək olar. Məsələn, kompüterlər üçün parollar siyasətininin təyin olunması, məlum təyinatdan sonra MS Windows Server 2003 əməliyyat sistemi dərhal bu siyasəti korporativ şəbəkənin kompüterlərində və ya konkret işçi stansiyasında tətbiq edir.

• **İstifadəçi məlumatlarının idarə edilməsi.** İstifadəçilər tərəfindən yaradılan faylları, sənədləri, elektron cədvəlləri və başqa informasiyaları idarə etmək üçün nəzərdə tutulubdur. İstifadəçilərin standart qovluqlarının məsələn, "My Documents" qovluğunu şəbəkə qovluğuna çevirərək və bu qovluğa avtonom rejimdə giriş hüququ verərək, istifadəçinin korporativ şəbəkənin ixtiyari nöqtəsindən bu qovluğa girişini təmin etmək olar.

• **İstifadəçi parametrlərinin idarə olunması.** Korporativ şəbəkələrdə hesablama mühitinin qruplar və ya ayrı-ayrı kompüterlər üçün mərkəzləşdirilmiş şəkildə idarə olunması məqsədini güdür. Korporativ şəbəkənin hər hansı bir kompüteri çökərsə, istifadəçi parametrlərini asanlıqla bərpa etmək mümkündür. İstifadəçi parametrlərinin tərkibində şəxsi tələblərdən doğan göstəricilərdən başqa, əməliyyat sisteminin və sistem proqramlarının interfeysləri tərəfindən təyin olunmuş göstəricilər də yer alır. İstifadəçi parametrlərinin tərkibində dilin seçilməsi, monitorun parametrləri və s. kimi göstəricilər iştirak edə bilərlər. İstifadəçi parametrlərinə korporativ şəbəkənin müxtəlif nöqtələrindən giriş əldə etmək mümkündür.

Proqram təminatlarının quraşdırılması və müşayiət olunması. Əməliyyat sisteminin yeniləşməsini, servis paketlərini, sistem proqramların pozulmasını və həmçinin sistemdə olan problemləri müəyyən etmək, sazlamaq kimi sistem funksiyalarını özündə cəmləşdirir. Korporativ şəbəkənin konkret istifadəçilər üçün müvafiq proqram təminatını təyin etmək, sadalanan funksiyalardandır. İstifadəçi üçün proqramların təyin olunması, istifadəçinin korporativ şəbəkənin hansı nöqtəsindən sistemə daxil olmasından asılı olmayaraq tam funksional şəkildə işləyəcəyini təmin edir. Burada proqramları kompüter üçün təyin etmək mümkündür. Bu halda isə proqram vasitələri müvafiq kompüterdə işləyən bütün istifadəçilər üçün əlçatan olacaq. Bu proqram antivirus və digər mühafizə vasitələri kimi sistem proqramların korporativ şəbəkənin bütün istifadəçiləri üçün istifadəsini xeyli asanlaşdırır. İstifadəçi üçün təyin olan sistem proqramın tələbə uyğun olaraq tam və ya natamam formasını kompüterə yükləmək olar. Əgər sistemdə proqram "tələb olunan zaman quraşdırılma" (on-demand install) göstəricisi ilə təyin olunubsa, onda bu proqram istifadəçinin ilk dəfə istifadəsi zamanı onun kompüterinə yüklənilәcək. Belə yanaşma çoxlu sayda istifadəçilər üçün işçi stansiyaların konfiqurasiyalarının tam açılmasını tezləşdirir. Lakin istifadəçilərin bir qismi bu və ya digər sistem proqramların tam imkanlarından istifadə etmirlər. Digər tərəfdən, MS Windows Server 2003 əməliyyat sistemində olan tam quraşdırılma variantı qrup siyasəti üçün istifadəyə çox yararlıdır. Administrator tərəfindən müəyyən olunmuş sistem proqramları istifadəçi aşağıdakı qaydada öz kompüterinə quraşdıra bilər:

Start→Settings→Control Panel→Add or Remove programs.

İstifadəçi və ya kompüter üçün təyin olunmuş sistem proqramlar korporativ şəbəkənin ixtiyari nöqtəsində istifadəçi tərəfindən quraşdırılıb istifadə edilə bilər. IntelliMirror vasitələri ayrı-ayrı və ya təşkilatın konkret tələblərindən asılı olaraq birgə tətbiq oluna

bilərlər. Korporativ şəbəkənin administratoru həm istifadəçinin parametrlərini, həm də verilənlərinin istifadə çərçivəsini məhdudlaşdıra bilər, yəni yalnız administrator tərəfindən müəyyən olunmuş kompüterlərdən istifadəçi öz parametrlərinə və ya verilənlərinə giriş əldə edə bilər. IntelliMirror vasitələri elə prinsiplə yaradılıb ki, bir sıra texniki üstünlüklərlə bərabər, həmçinin, korporativ şəbəkəni idarə edilməsində xərclərin də azalmasını özündə ə ks etdirir. IntelliMirror vasitələrinin böyük hissəsi istifadəçilərin məhsuldar işinin və mərkəzləşdirilmiş idarəetmənin təşkil olunmasına yönəlmişdir. Bu da öz növbəsində administrativ müdaxilələrin qarşısının alınması vasitəsi ilə korporativ şəbəkəni idarə edilməsində xərclərin azalmasına gətirib çıxarır. IntelliMirror vasitəsi tərəfindən təklif olunan mərkəzləşdirilmiş idarəetmə təşkilatlara daha az xərclə onlara məxsus korporativ şəbəkələrdə dəyişiklikləri və konfiqurasiyaları idarə etmək imkanını yaradır. Çünki bütün təşkilatın korporativ şəbəkəsi Active Directory vasitəsi ilə idarə oluna bilər.

5.8 Korporativ şəbəkənin təhlükəsizlik və istifadəçi siyasətinin idarə olunması

"Group Policy Management Console" (GPMC) vasitəsi, MS Windows Server 2003 əməliyyat sisteminə əlavə genişlənmə kimi təklif olunur və qrup siyasətinin idarə olunmasının yeni strukturunu təklif edir. Korporativ şəbəkədə GPMC vasitəsi ilə qrup siyasətini tətbiq etmək daha rahat və asandır. Belə olan halda Active Directory vasitəsini də istifadə etmək daha effektiv olar.

Beləliklə GPMC vasitəsi GPO təchizatının ehtiyat surətinin çıxarılmasını və bərpasını, GPO təchizatının idxal/ixrac, GPO təchizatının parametrlərini və "Resultant Set of Policy" (RSoP) verilənləri haqqında hesabatın generasiyasını, konfiqurasiyanın idarə edilməsi üçün şablonların tətbiq olunmasını və həmçinin ssenariyə əsasən GPMC vasitəsinin bütüm əməliyyatlarını idarə edilməsini təmin edir.

Digər tərəfdən GPMC bir neçə domenlərin siyasətinin və bir altşəbəkədə yerləşən saytların idarə olunmasına imkan yaradır və bunun üçün "drag-and-drop" texnologiyasını dəstəkləyən sadələşdirilmiş istifadəçi interfeysi təklif edir. Əgər altşəbəkələr qarşılıqlı etibar münasibətləri şəklində əlaqələndirilibsə, onda korporativ şəbəkənin administratoru bir konsol vasitəsi ilə bir neçə altşəbəkənin qrup siyasətini idarə etmək imkanına qadir olur. GPMC vasitəsi, MS Windows Server 2003 əməliyyat sisteminin domenlərində qrup siyasətini idarə etmək imkanına malikdir. Lakin qrup siyasətinin obyektləri bir altşəbəkə çərçivəsində cəmləşən saytlar vasitəsi ilə domenlə ə laqədə ola bilərlər. MS Windows. NET Server əməliyyat sisteminində altşəbəkələr arasında olan etibarlı idarəetmə münasibətləri, qrup siyasətlərini bir sıra yeni ssenarilər vasitəsi ilə realizə etməyə imkan verir.

"X" altşəbəkədən olan istifadəçi özünə məxsus siyasət qaydaları olan "Y" altşəbəkəsinə daxil ola bilər. GPO parametrləri alternativ olaraq digər altşəbəkələrə müraciət edə bilər. Bu ssenari elementləri MS Windows Server 2003 əməliyyat sisteminin qrup siyasəti tərəfindən dəstəklənir. "RsoP" aləti qrup siyasətinin kompüterə və ya istifadəçiyə tətbiq olunma effektini qiymətləndirməyə imkan verir. "RsoP" aləti, qrup siyasətinin planlaşdırılması, idarə olunması və sazlanmasında olan problemlərin nizamlanması funksiyalarını yerinə yetirir. "RsoP" – "MMC" təchizatı çərçivəsində reallaşdırılan həm infrastruktur, həm də alətdir. Onun vasitəsi ilə qeydiyyat və planlaşdırma rejimində cari siyasətin parametrlərini təyin və analiz etmək mümkündür.

İlkin olaraq sistemin siyasətini verilmiş məqsədə tətbiq olunmasının cari nəticələrini müşahidə etmək olur, ikincisi – qrup siyasətinə real dəyişikliklərin olunması zamanına qədər, dəyişikliklərin mümkün olan nəticələrinin müşahidə etmək imkanı yaradır. "RsoP" aləti "WMI" (Windows Management Instrumentation) vasitəsi verilənlərinin müxtəlif nöqtələrdən

yığılması bacarığından istifadə edə bilir. "MMC" mühitində işləyən alət məqsədli obyektdən asılı olaraq nəticələrin nümayiş olunması üçün təchizatın genişlənməsini dəstəkləyir. Məqsədi təyin edən avtomatlaşdırılmış sistem, "RsoP" alətinin təsir aralığını təyin edir. Bu avtomatlaşdırılmış sistem, administratoru məqsədli obyektin yaradılması, "RsoP" verilənlərinin generasiyası və bu verilənləri istifadə etmək məqsədi ilə RSoP alətinin işə salınması üçün bütün mərhələlərdən keçirəcək.

"WMI" vasitəsi, məqsədli kompüter üçün böyük həcmli informasiya generasiya edir. Məsələn, aparat və proqram təminatlarının siyahısı, konfiqurasiya parametrləri. İnformasiya mənbəyi kimi "WMI" vasitəsi reyestrdən, drayverlərdən, fayl sistemindən, Active Directory, Simple Network Management Protocol (SNMP), Windows Installer xidmətindən, SQL proqramlaşdırma dilindən və Exchange Server proqramından istifadə edir. Windows Server 2003 əməliyyat sistemində "WMI Filtering" funksiyası dinamik olaraq "WMI" verilənlərinə olan müraciətlər əsasında GPO təchizatını tətbiq edilməsi qərarının qəbul edir. Bu müraciətlər korporativ şəbəkənin GPO təchizatında göstərilən hansı kompüterlərin və istifadəçilərin siyasətin parametrləri ilə təmin olunacağı təyin edir. Bu funksionallıq lokal kompüter xassələri əsasında qrup siyasətinin məqsədlərini avtomatik şəkildə təyin etmək üçün tam şərait yaradır.

Aşağıda "WMI Filtering" funksiyasını yaratmaq üçün müxtəlif xassələrin nümunələri verilmişdir:

- **xidmətlər:** DHCP (Dynamic Host Configuration Protocol) protokolunu dəstəkləyən kompüterlər;
- **reyestr:** reyestrində əvvəlcədən müəyyən edilmiş bölmələri dolu olan kompüterlər;
- **aparat vasitələri:** prosessorun tipi ən azı Pentium IV olan işçi stansiyalar;
- **proqram vasitələri:** "Visual Studio.NET" proqram təminatı olan işçi stansiyalar;

• **aparat konfiqurasiyası:** 3-cü səviyyəni dayanmadan istifadə edən şəbəkə kartlı işçi stansiyalar;
• **proqram konfiqurasiyası:** qrup şəklində göndərmələri (multicasting) aktiv olan işçi stansiyalar;
• **asılılıqlar:** SNA (systems network architecture) xidmətindən asılı olan xidmətlərlə təchiz olunan işçi stansiyalar;
• **ping əmri**: "ping" komandası vasitəsi ilə əvvəlcədən müəyyən olunmuş serverə exo-paketlərin ötürülməsinə 100 millisaniyədən az zaman sərf edən işçi stansiyalar;

Veb-rejiminin qrup siyasəti obyektlərinin redaktoruna inteqrasiya olunması anlaşılmanı, idarəetməni və cari informasiya texnologiyaları siyasətin parametrlərinin qiymətləndirilməsini asanlaşdırır. Sistemin siyasətini təmsil edən siyasət ilk növbədə əməliyyat sisteminin hansı platformalarla, proqram-aparat təminatları ilə birgə qüsursuz işləməsini nəzərdə tutur. Belə yanaşma zamanı sistem siyasətinin elementləri dərhal anlaşılır və məqsədə çatmaq üçün ən qısa yollardan biri kimi praktikada dəyərləndirilir. MS Windows Server 2003 əməliyyat sisteminin ailəsində sistemə məxsus çox sayda təhlükəsizlik, idarəetmə və çevikliyi təmin edən siyasət qaydaları toplusu mövcuddur. MS Windows Server 2003 əməliyyat sistemi özündə 160-dan çox yeni siyasət qaydalarını cəmləşdirir. Bu qaydalar vasitəsi ilə aşağıda sadalanan komponentlərinin idarə olunması nəzərdə tutulmuşdur:
• Terminal Server;
• proqram təminatlarının uyğun gəlməsi;
• şəbəkənin dəstəklənməsi, SNMP, xidmətin keyfiyyəti (QoS), mühafizə sistemləri və icazələrin idarə olunması;
• DNS-də qeydiyyatı;
• istifadəçi profilləri və qrup siyasəti;
• idarəetmə paneli;
• Windows Media Player.

"Supported" sözünü idarəetmə şablonuna (.adm) daxil etməklə, siyasətin hər bir qaydası üçün onların hansının MS Windows Server 2003 əməliyyat sistemi və konkret servis paketləri tərəfindən dəstəkləndiyini müəyyən etməyə imkan verir. Administrator və həmçinin istifadəçilər əməliyyat sistemi tərəfindən tanınanları görmək şərti ilə bu "açar sözləri" vasitəsi ilə siyasətin qaydalarını axtarmaq hüququna malikdirlər. Hər bir qaydaya uyğun izahedici mətn onun hansı əməliyyat sistemini dəstəkləmək imkanına malik olduğu ilə başlayır.

İstifadəçi verilənlərinin idarə olunması. Verilənlərə daimi girişin olması – korporativ şəbəkələrin əsas amillərindən biridir. IntelliMirror vasitələri korporativ şəbəkənin ixtiyari istifadəçisinin şəxsi verilənlərinə həm operativ rejimdə, həm də avtonom rejimdə şəbəkənin ixtiyari nöqtəsindən giriş əldə etməyə imkan verir. Korporativ şəbəkənin administratoru verilənlərin arxivlərini mərkəzləşdirilmiş şəkildə idarə etmək imkanına malikdir. Bu isə öz növbəsində sıradan çıxmış işçi stansiyalarını asanlıqla əvəz etməyə şərait yaradır. İstifadəçilər korporativ şəbəkənin ixtiyari MS Windows XP Professional əməliyyat sistemi olan kompüterindən şəxsi verilənlərinə giriş əldə edə bilərlər. İstifadəçinin verilənləri şəbəkədə xüsusi ayrılmış bir qovluqda yerləşdirilir. Əlçatan qovluqların və verilənlərin siyahısını heç bir xüsusi vasitə istifadə etmədən qrup siyasəti vasitəsi ilə sazlamaq olar. Əgər istifadəçi şəbəkədə saxlanılan şəxsi resursları ilə avtonom rejimdə işləyirsə, onda onun verilənləri avtomatik şəkildə şəbəkəyə yenidən qoşulduqda şəbəkədə olan resursları ilə sinxronlaşacaq. İstifadəçi verilənlərinin idarəetmə vasitələri onların hər zaman əlçatan olmağına təminat verir:

- administratorlar istifadəçi verilənlərini ümumi şəbəkə kataloquna yönəldərək və ya ehtiyat nüsxə çıxararaq daha etibarlı mühafizə edə bilərlər. Belə yanaşmada istifadəçi verilənlərini mərkəzləşdirilmiş ehtiyat nüsxəsi administratorun tam nəzarəti

altında həyata keçirilir. Bu isə istifadəçi verilənlərinin mərkəzi fayl serverinə köçürülməsi kimi korporativ qaydaların reallaşmasına imkan yaradır.

• administratorlar həm korporativ şəbəkənin mərkəzi fayl serverində, həm də lokal istifadəçi kompüterində verilənlərin aktual versiyasının olmasına təminat verir. Lokal keşlənmə əməliyyatı hətta kompüter şəbəkəyə qoşulmadığı və ya avtonom rejimdə işlədiyi halda belə lokal kompüterdə verilənlərlə işləməyə imkan verir.

• istifadəçi digər kompüterə keçdikdə, verilənlər onunla bərabər həmin kompüterə transfer olunurlar. Bunun nəticəsində də istifadəçinin çevikliyi və iş fəaliyyətinin rahatlığı təmin olunur. İstifadəçi öz informasiya resurslarına korporativ şəbəkənin ixtiyarı nöqtəsindən giriş əldə edə bilər.

Qrup siyasəti istifadəçinin "My Documents" qovluğunu onun öz şəxsi kataloquna yönəldilməsinə imkan yaradır. Bu isə öz növbəsində korporativ şəbəkənin istifadəçilərinin köhnə tip şəxsi kataloqlarından, yeni tip kimi tanınan "My Documents" qovluğuna keçidini və köhnə tip şəxsi kataloqla tam uyğunlaşmasını təmin edir. İstifadəçi verilənlərin idarə edilməsini reallaşdırmaq üçün aşağıda göstərilən texnologiyalardan istifadə etmək imkanına malikdir:

• Active Directory;
• qrup siyasəti;
• RSoP;
• istifadəçi profilləri;
• qovluqların yönəldilməsi;
• avtonom fayllar;
• sinxronlaşdırma dispetçeri;
• Distributed File System (DFS);
• Encrypting File System (EPS);
• disk fəzasının kvotaları.

İstifadəçi parametrlərinin idarə olunması. İstifadəçi parametrlərinin idarə olunmasına imkan verən IntelliMirror vasitəsi, administratorlara mərkəzləşdirilmiş şəkildə qrup istifadəçiləri və kompüterlər üçün onların avtomatik konfiqurasiya olunması məqsədi ilə parametrlərini təyin etmək üçün imkan yaradır. Bundan başqa korporativ şəbəkənin administratorları işçi stansiyaların sıradan çıxması zamanı istifadəçi parametrlərini bərpa edə bilər və həmçinin istifadəçinin yerini korporativ şəbəkə çərçivəsində dəyişdikdə, onunla bərabər parametrlərinin də yerini dəyişə bilər. Şəbəkə administratorları aşağıda sadalanan funksiyaları yerinə yetirə bilərlər:

- işçi stansiya üçün əvvəlcədən təyin olunmuş mühiti təqdim etməklə, texniki şöbənin mütəxəssislərinə müraciətlərin sayının azaldılması;
- işçi stansiyalar sıradan çıxdığı zaman, onların dəyişdirilməsinə itirilən vaxt və məsrəflərin azaldılması;
- istifadəçilərin korporativ şəbəkənin hansı nöqtəsindən sistemə daxil olmasından asılı olmayaraq onların işçi parametrlərinin eyni qaydada korporativ şəbəkənin ixtiyari kompüterinə yüklənməsi vasitəsi ilə istifadəçilərin iş fəaliyyətinin effektivliyinin artırılması.

Burada həmçinin istifadəçinin profilini (təhlükəsizlik, dil, ssenarilər sistem proqramlar və s.) idarə etmək mümkündür. Bu informasiya bütün istifadəçilər üçün korporativ şəbəkədə heç olmasa bir dəfə işləmiş hər bir kompüterdə saxlanılır. Eyni zamanda istifadəçi qovluqlarını şəbəkə diskinə yönəltmək olar. Bu isə öz növbəsində istifadəçinin korporativ şəbəkəyə hansı kompüterdən daxil olduğundan asılı olmayaraq vahid bir profilini qorumağa imkan yaradır. İstifadəçinin profili də onun verilənləri kimi istifadəçinin hansı kompüterdə işləməsindən asılı olmayaraq, onunla birgə şəbəkə çərçivəsində hərəkət edir. Qrup siyasətinin parametrləri administratorlara istifadəçinin əhatə dairəsini də idarə etməyə imkan verir. Lakin istifadəçiyə əhatə dairəsini idarə etmək hüququ vermir. Bəzi hüquqlara malik olmaqla istifadəçilər

özlərinə xas şəkildə bu mühitin müəyyən elementlərini dəyişdirə bilərlər. Parametrlər əsasən üç tip informasiyaya malikdirlər:

- İstifadəçi və administrativ informasiya;
- Müvəqqəti informasiya;
- Lokal kompüter üçün spesifik olan verilənlər.

Adətən müvəqqəti və lokal verilənlər istifadəçinin arxasınca korporativ şəbəkədə yerini dəyişməməlidir. Onların yerlərinin dəyişməsi korporativ şəbəkənin dəstəklənməsində artıq xərclərə və itkilərə yol açа bilər. Kompüterlərin müxtəlifliyi isə bu informasiyaların qarşılıqlı mübadiləsinin qabağını ala bilər. Əgər "rouminq" (roaming) istifadəçi profili tətbiq olunubsa, onda qrup siyasəti, yalnız ən vacib istifadəçi və adminstrativ verilənlərin yadda saxlanılacağına, müvəqqəti və ya lokal parametrlər isə lazım gəldikdə, yenidən dinamik şəkildə generasiya olacağına təminat verir. Belə yanaşma korporativ şəbəkə daxilində saxlanılan və ötürülən informasiyanın həcmini azaldaraq, istifadəçilərə oxşar və ya uyğun iş mühitini şəbəkənin ixtiyari kompüterində yaradılmasına imkan verir.

İstifadəçi parametrlərinin idarə olunması üçün aşağıda sadalananlar istifadə olunurlar:

- Active Directory;
- qrup siyasəti;
- avtonom fayllar;
- sinxronlaşdırma dispetçeri;
- DFS;
- qovluqların yönəldilməsi;
- "rouminq" istifadəçi profilləri .

MS Windows Server 2003 əməliyyat sistemi bir sıra yeni siyasət qaydalarını özündə cəmləşdirir. Onların vasitəsi ilə istifadəçilərə profillərini çevik konfiqurasiya etməyə, bəzi kompüterlərdə bu profillərin söndürülməsinə və dəyişilməz profillərin yaradılmasına imkan verir.

5.9 Korporativ şəbəkələrdə proqram vasitələrinin idarəçiliyi

İstifadəçilərin proqram təminatı ilə təmin edilməsinin praktik baxımdan bəzi problemləri mövcuddur:

• istifadəçilərə müxtəlif proqram təminatları tələb olunur, məhz bu səbəbdən böyük təşkilatlarda yüzlərlə proqram təminatını dəstəkləyən sistemlər çalışır. Belə korporativ şəbəkənin administratorları bu proqram təminatlarının effektiv və qüsursuz işləməsinin və quraşdırılmasını təşkil etməlidirlər.

• müəyyən zaman keçdikdə proqram təminatları köhnəlməyə başlayırlar və yeni versiyalar və ya tam yeni proqram təminatı aktuallaşır. Belə halda istifadəçi şablonlarının və ya servis paketlərinin yeni versiyalarını sistemə quraşdırmaq və ya yeniləşdirmə əməliyyatı vasitəsi ilə bu proqramları gündəmə uyğun saxlamaq lazımdır.

• iş əsnasında vaxtaşırı işçilərin yeni proqramlara ehtiyacı yaranır və bununla yanaşı bəzi köhnə proqram təminatları öz aktuallığını itirirlər. Digər tərəfdən istifadəçi korporativ şəbəkənin ixtiyari kompüterindən sistemə qoşulduqda ona öz istifadə etdiyi proqram təminatı lazım ola bilər.

Əgər istifadəçiyə lazım olan bütün proqram təminatları əlçatan olarsa, onda istifadəçinin məhsuldarlığı da artar. Administrator artıq istifadəçiyə lazım olmayan və köhnəlmiş sayılan proqram təminatlarını vaxtı-vaxtında silinməsini təmin etməlidir. Odur ki, hansı proqram təminatlarının istifadəsinin dayandırılmasının və ya hansının yeniləşdirilməsinin vacibliyi texniki şöbə tərəfindən təyin olunur. Bəzən köhnəlmiş proqram təminatlarını silmək, onun uyğunlaşması ilə mübarizə etməkdən daha məqsədə uyğundur. Bir çox təşkilatlar böyük qruplara və ya korporativ şəbəkənin bütün istifadəçilərinin işçi stansiyalarına məxsus proqram təminatlarının idarə olunmasını avtomatlaşdırmağa çalışırlar. IntelliMirror vasitəsi proqram təminatlarının quraşdırılması və dəstəklənməsi üçün kompüteri işə salan zaman, yəni istifadəçinin sistemə daxil olduğu vaxtda

proqram təminatlarının yüklənməsinə imkan yaradır. Bu vasitələri həmçinin proqram təminatlarının yeniləşdirilməsi, lazımsız olan proqramların silinməsi, servis paketlərinin açılması və əməliyyat sisteminin yeniləşdirilməsi məqsədi ilə istifadə etmək olar. Həmçinin bu halda istifadəçi tərəfindən heç bir proqram təminatını diskdən və ya başqa informasiya daşıyıcısından kompüterə yükləyə bilməyəcəyinə təminat vermək olar.

IntelliMirror vasitəsi aşağıda göstərilən vəziyyətlərdən çıxış yolları təklif edir:

• əgər istifadəçi proqram təminatının sistem faylını bilmədən pozubsa, onda həmin fayl avtomatik bərpa olunacaq;

• istifadəçinin korporativ şəbəkənin digər kompüterinə keçdikdə onun bütün proqram təminatları tam şəkildə yeni kompüterdə açılacaq;

• əgər istifadəçi işlədiyi kompüterdə olmayan proqramın faylını açmağa cəhd göstərirsə, onda bu proqram avtomatik olaraq kompüterə yüklənib, açılması tələb olunan faylı tam şəkildə açacaqdır.

Qrup siyasəti proqram təminatının quraşdırılması parametrlərini və hansı komponentləri quraşdırmaq, silmək və ya yeniləşdirmək lazım olduğunu təyin etməyə imkan verir. Proqram təminatının quraşdırılması siyasətinin qaydaları bütün qrup istifadəçilərinə və ya kompüterlərinə tətbiq oluna bilər. İstifadəçi kompüterlərinə proqram təminatının quraşdırılmasının iki metodu mövcuddur:

— təyinetmə (assigning)

— nəşretmə (publishing).

• **Təyinetmə**

Qrup siyasəti proqram təminatlarını hər hansı bir istifadəçiyə və ya kompüterə təyin etməyə imkan verir. Kompüterə təyin olunmuş proqram təminatları kompüterin növbəti dəfə işə salınma zamanı yüklənməyə başlayacaqlar. İstifadəçiyə administrator tərəfindən proqram təminatlarının təyin olunması zamanı "tələb olunan

zaman quraşdırılma" (on-demand install) və ya "tam quraşdırılma" (full install) funksiyaları təyin edilə bilər.

* *Tələb olunan zaman*

Əgər proqram təminatlarının "tələb olunan zaman quraşdırılma" təyin olunubsa, onda istifadəçi kompüterində hökmən "Start" menyusunda bir bənd əlavə olunur və reyestrdə fayllar tipi arasında müvafiq əlaqələr yaradılır. İstifadəçiyə hər şey elə təqdim olunur ki, sanki proqram təminatı artıq kompüterə yüklənib, quraşdırılmışdır. Lakin proqram təminatı istifadəçi tərəfindən tələb olunmayana qədər tam şəkildə quraşdırılmır. İstifadəçi kompüterdə proqram təminatının və ya onunla əlaqədar olan bir faylın açılmasına cəhd etdikdə, "Windows Installer" vasitəsi proqram təminatının düzgün işləməsi üçün sistem tərəfindən tələb olunan bütün fayl və parametrlərinin mövcudluğunu yoxlayır. Əgər onlar yoxdursa, "Windows Installer" vasitəsi onları əvvəlki paylama məntəqəsindən qəbul edib quraşdıracaq.

* *Tam quraşdırılma*

Bu rejim iş yerində stabil olmayan bir sıra istifadəçilər üçün çox rahatdır. Bu rejimdə istifadəçinin proqram təminatı onun sistemə daxil olduğu zaman kompüterə yüklənir və quraşdırılma prosesinə başlanılır. Proqram təminatlarının əvvəlcədən təyin olunma funksiyası istifadəçinin hərəkətlərindən asılı olmayaraq, onun bu proqramlara əlyetənliyi təmin olunur. Əgər təsadüf nəticəsində və ya qəsdən istifadəçi siyahıda təyin olunmuş proqramlardan birini və ya bir neçəsini pozubsa, onda bu proqramlar avtomatik şəkildə kompüterə növbəti giriş zamanı yüklənib quraşdırılacaq.

• **Nəşretmə**

Nəşretmə əməliyyatı zamanı proqram vasitəsi İdarəetmə Panelinin "Add or Remove Programs" bəndində əks olunur. İstifadəçilər nəşr olunmuş proqram vasitələrini buradan quraşdıra bilərlər. Proqrama uyğun faylı açdığımız zaman quraşdirilma prosesini avtomatik şəkildə başlamasını təmin etmək olar. İstifadəçi üçün hər hansı bir proqramın çox da önəm kəsb etmədiyi hallarda nəşr

etmə əməliyyatı tətbiq olunur. Nəşretmə əməliyyatının əhəmiyyətli bir vasitə olmasını ancaq o zaman başa düşmək olar ki, bütün nəşr edilmiş proqram vasitələrinin quraşdırılması "Windows Installer" vasitəsinin köməyi ilə reallaşsın. Burada ".zap" fayllarını tətbiq etməklə "Windows Installer" vasitəsini dəstəkləməyən proqram təminatlarının nəşr olunması da mümkündür. Lakin bu zaman "Windows Installer" vasitəsinin quraşdırılma prosesində təklif etdiyi bir sıra üstünlüklərindən yararlanmaq mümkün olmayacaq.

Mətn faylı olan ".zap" distributiv göstəriciləri özündə saxlayır və proqram vasitəsinin "Add or Remove Programs" bəndində əks olunmasını təmin edir. Qrup siyasaətinə əsasən hər hansı bir proqram vasitəsinin açılması prosesi "Windows Installer" vasitəsini avtomatik olaraq tələb edir. Belə olan halda "Windows Installer" vasitəsi nəinki proqram təminatının kompüterə yazmaq prosesini, həm də proqramın lokal fayllarının tamlığının təsadüfü yarana bilən ziyanlardan qorunmasını təmin edir.

Məsələn, əgər istifadəçi bir neçə sistem faylı çatmayan MS Word proqramında işləmək istəyirsə, onda "Windows Installer" vasitəsi avtomatik olaraq həmin faylları quraşdırılma məntəqəsindən dərhal MS Word proqramının ikinci dəfə açmaq cəhdi zamanı quraşdırır. Bundan başqa "Windows Installer" vasitəsini dəstəkləyən proqram vasitələrini qrup siyasəti çərçivəsində bir sıra üstünlüklərlə quraşdırmaq mümkündür. Bu isə öz növbəsində o deməkdir ki, istifadəçilər administrator tərəfindən müəyyən olunmuş hər hansı bir proqram təminatını öz kompüterlərinə yazdığı zaman, heç də həmin kompüterin administratoru hüququna malik olmalı deyillər. İxtiyari proqram təminatının bərpa prosesi ehtiyac yaranan zaman proqramın quraşdırılması ilə eyni alqoritmə malikdir. "Windows Installer" vasitəsi quraşdırılmış kompüterlər hər dəfə proqram təminatını açdığı zaman bir neçə vacib sistem fayllarının varlığını yoxlayır. Əgər fayl və parametrlərin bərpası lazım olarsa, onda onlar avtomatik

şəkildə bərpa olunacaqlar. MS Windows Server 2003 əməliyyat sistemi proqram təminatının açılması üçün digər yeni təkmilləşmələr də təklif edir.

İstifadəçinin sistemə daxil olduğu zaman təyin olunmuş proqram vasitələrinin tam quraşdırılması. Proqram təminatı quraşdırılması vasitəsi "Software Settings" bölməsində yerləşən "Group Policy Object Editor" qaydası daha da təkmilləşdirilmişdir və yeni sayılan proqramların "tam quraşdırılması" bəndi əlavə olunmuşdur. Bu vasitənin köməyi ilə istifadəçi üçün təyin olunmuş proqram vasitələrini sistemə daxil olan zaman tam şəkildə quraşdırmaq olar. Tam quraşdırılma rejimi tez-tez iş yerini səfərlərlə əlaqədar tərk edən və bu zaman bütün proqram vasitələrinin tam şəkildə quraşdırılmasına ehtiyacı olan qrup istifadəçiləri üçündə çox sərfəli və rahatdır.

64-bitlik proqramların dəstəklənməsi. Proqram quraşdırılmasının yeni parametrləri qrup siyasəti çərçivəsində 32-bitlik proqram təminatlarını 64-bitlik kompüterlərə yazılmasının icazəsini idarə etməyə imkan verir.

MS Windows Server 2003 əməliyyat sistemi üçün olan funksionalliğin təmin olunması MS Windows 2000 Server əməliyyat sistemi üçündə eyni səviyyədə keçərlidir. Bu imkan o zaman yararlı olur ki, korporativ şəbəkənin administratoru 32-bitlik "Windows Installer" paketini 64-bitlik sistemlə işləyən istifadəçi kompüterlərinə yazmağı planlaşdırır. Yeni olan "Make 32-bit x86 Windows Installer Application Available To IA64 Machines" və "Group Policy Software Installation" bəndində yerləşən funksiyanı seçməklə 32-bitlik paketin 64-bitlik sistemlə işləyən istifadəçi kompüterlərində qüsursuz işləməsi praktik baxımdan tam məqsədə uyğundur.

Quraşdırılma prosesini reallaşdırmaq və proqram vasitələrinin müşayiət olunması üçün aşağıda sadalanan Windows əməliyyat sistemi ailəsinə məxsus texnologiyalar istifadə olunur:

• Active Directory;

• qrup siyasəti;
• Windows Installer;
• Add/Remove aləti;
• DFS;
• faylların replikasiya xidməti (File Replication Service - FRS).

Yeni işçi stansiyanın quraşdırılması. Əgər korporativ şəbəkənin hər hansı bir istifadəçisinə yeni işçi stansiya tələb olunursa, onda bu şəbəkənin administratorunun informasiya texnologiyaları siyasətinin nizamnaməsinə görə atacağı addımlar aşağıdakılardır:
• istifadəçiyə çox qısa zamanda öz işçi vəziyyətinə qayıtmağa imkan yaratmaq;
• texniki şöbənin mütəxəssislərinin yeni istifadəçi tərəfindən çox və ya müntəzəm çağırılmasının qarşısının alınması və bu müraciətlərin sayını tam minimuma endirmək.

Bu göstəricilərin müsbət şəkildə həyata keçirmək üçün məsafədən idarəetmə (Remote Installation) tam yardımçı ola bilər. Bütün prosedura yalnız korporativ şəbəkənin informasiya texnologiyaları siyasəti üzərində qurulub və işçi kompüterində çalışmadan bu əməliyyatları yerinə yetirmək olar.

"Remote Installation" vasitəsini korporativ şəbəkənin "Pre-Boot eXecution Environment" (PXE) xidmətini dəstəkləyən bütün müştəri-kompüterlərində MS Windows əməliyyat sisteminin ilk quraşdırılması zamanı istifadə etmək olar. Korporativ şəbəkənin informasiya texnologiyaları siyasətinə uyğun əməliyyat sisteminin və əsas proqram vasitələrinin quraşdırılması üçün administratorun yeni quraşdırılacaq işçi stansiyanın qoşulduğu nöqtəyə getməsinə ehtiyac qalmır. Belə halda korporativ şəbəkənin administratoru məsafədən quraşdırılmanı təşkilatın informasiya texnologiyaları siyasətinin tələblərinə uyğun tam avtomatlaşdıra bilər. Beləliklə, istifadəçi öz kompüterini ilk işə saldığı zaman klaviaturadan "F12" düyməsini basaraq korporativ şəbəkənin administratoru tərəfindən təyin

olunmuş quraşdırılma prosesini başlatmış olur. Sonra işçi stansiya "RIS" (Remote Installation Services) xidmətini dəstəkləyən şəbəkə serverindən yüklənir. İstifadəçi sistemə daxil olduqdan sonra "RIS" xidməti aşağıdakı elementlərin quraşdırılmasında əvəzləyici rol oynaya bilər:

• MS Windows əməliyyat sisteminin distributiv diskinin şəbəkə ekvivalenti;

• əməliyyat sisteminin obrazı əvvəlcədən konfiqurasiya edilmiş proqram təminatlarını, yəni mətn prosessorlarını və ya elektron poçt proqramlarını quraşdırmaq imkanına malikdir.

Məsafədən quraşdırılma xidmətini reallaşdırmaq üçün aşağıda sadalananlar istifadə olunacaqdır:

• Active Directory;
• Qrup siyasəti;
• DNS;
• DHCP;
• RIS.

Lakin əməliyyat sisteminin bir sıra xidmətləri də mövcuddur ki, onlar komanda sətri vasitəsi ilə həyata keçirilir. Komanda sətri, müntəzəm yerinə yetirilməsi vacib olan hərəkətləri avtomatlaşdırmağa, çap serverləri, "Internet Information Services" (IIS) xidməti və Active Directory xidməti kimi vacib əhəmiyyətli komponentlərin idarə edilməsinə imkan verən 60-dan çox yeni əmrlərdir.

Bu əmrlərin təklif etdiyi üstünlüklər bunlardır:

İstifadəyə hazırlıq. İstifadəsi üçün heç bir əlavə proqramlaşdırma kodu lazım olmayan və ya çox cüzi həcmdə kod tələb edən hazır həllər təklif olunur. Bütün əmrlərin komanda sətrində yazılma sintaksisi vahid şəkildədir və komanda sətrinə asan bir formada daxil edilə bilir. Komanda sətri xidmətinin istifadəsi haqqında kömək məqsədi ilə ayrıca HTML-formasında (ntcrnds.chm) xidmət mövcuddur. Bu xidməti menyudan "Help and Support Center" bəndini seçərək aktivləşdirmək olar.

Bütün yeni əmrlər "/s" parametri vasitəsi ilə məsafədə yerləşən serverlə işi dəstəkləyir. "Telnet" və "Terminal Services" mühitlərində işləmək qabiliyyətinə malikdir və məsafədə yerləşən serverin adını müəyyən etməyə imkan verir. Belə yanaşma məsafədən idarəetmə prinsiplərini komanda sətri vasitəsi ilə reallaşdırmağa tam imkan verir.

Komanda sətrindən, komanda tipli faylları və ya xüsusiləşdirilmiş idarəetmə əməliyyatlarının ssenarisini və müntəzəm yerinə yetirilən əməliyyatların avtomatlaşdırılmasını işə salmaq mümkündür.

Komanda prosessoru. Komanda prosessoru – istifadəçilərin əməliyyat sistemi ilə qarşılıqlı əlaqəsini təmin edən ayrıca bir proqramdır. Komanda prosessorunun qrafik olmayan interfeysi konsol proqramlarının və əmrlərinin yerinə yetirilməsi mühitini təqdim edir. Komanda prosessoru proqramları yerinə yetirir və onların işi nəticəsində meydana gələn verilənləri simvol şəklində ekranda təsvir edir. Belə görünüş həm də MS DOS əməliyyat sisteminin komanda prosessoru olan "Command.com" vasitəsinə oxşayır. MS Windows Server 2003 əməliyyat sistemi komanda prosessoru əvəzinə komandalar interpretatoru olan "Cmd.exe" vasitəsini istifadə edir. "Cmd.exe" vasitəsi öz növbəsində sistem proqramları yükləyir və onlar arasında informasiya axınlarının ötürülməsini və istifadəçinin daxil etdiyi məlumatı əməliyyat sisteminin başa düşə biləcəyi formaya keçirilməsini təşkil edir. Komanda prosessorunun təkmilləşdirilməsi idarəetmənin effektivliyinə birbaşa təsir göstərir. Beləliklə, komanda prosessorunu aşağıda sadalananların həyata keçirilməsi üçün istifadə etmək olar:

• komanda prosessorunun gündəlik standart işini avtomatlaşdıran komanda fayllarının yerinə yetirilməsi üçün istifadəsi. Məsələn, ssenari vasitəsi ilə gecələr fayl sisteminin və ya elektron poçt qutularını arxivləşdirmə əməliyyatını yerinə yetirmək olar;

• komanda prosessoru mühitində daha ciddi ssenarilərin yerinə yetirilməsinə imkan verən "Cscript" vasitəsinin "Windows Script Host" versiyasını komanda sətri üçün istifadə etmək olar;
• əməliyyatların yerinə yetirilməsinin effektivliyinin artırılmasına istifadəçi interfeysi əvəzinə komanda faylı tətbiq edilməsi. Komanda faylının tərkibində komanda sətrində mümkün olan bütün komandaları istifadə etmək olar;
• proqram təminatlarının yerinə yetirilməsinə tam nəzarət etmək baxımından komanda sətri pəncərəsinin tərkibinə baxış rejiminin quraşdırılması.

Komanda sətrinin əmrləri. Aşağıda MS Windows Server 2003 əməliyyat sisteminin komanda sətrinin yeni və bir sıra vacib əmrlərinin siyahısı verilmişdir:
• **adprep** – MS Windows 2000 Server əməliyyat sistemindən MS Windows Server 2003 əməliyyat sisteminin Standard Edition, Enterprise Edition və ya Datacenter Edition versiyalarına keçid zamanı domen və ya altşəbəkələri hazırlayır;
• **bootcfg** – "Boot.ini" faylının parametrlərini dəyişdirmək, nəzərdən keçirmək və konfiqurasiyasına dəyişiklik etmək imkanı verir;
• **choice** – kömək sətri vasitəsi ilə istifadəçiyə seçim etmək imkanı verir və istifadəçi təklif olunan variantlardan birini seçməyənə qədər proses öz işini müvəqqəti dayandırır;
• **clip** – komanda sətri pəncərəsində əmələ gələn informasiyanı sistem buferinə yönəldir;
• **cmdkey** – yadda saxlanılmış istifadəçi adlarını və parollarını yaradır, təsvir edir və pozur;
• **defrag** – lokal disklərin tomlarında yüklənmə fayllarının, verilənlərin və qovluqların defraqmentasiyasını yerinə yetirir;
• **diskpart** – disklər və bölmələri idarə edir;
• **driverquery** – drayverlərin siyahısını çıxartmağa imkan verir;
• **dsadd** – kompüter, kontakt, qrup, təşkilatı bölməni və nəhayət istifadəçini Active Directory servisinə əlavə edir;

• **dsget** – Active Directory servisində olan kompüterin, kontaktın, qrupun, təşkilatı bölmənin, istifadəçinin və serverin seçilmiş atributlarını göstərir;
• **dsmod** – Active Directory servisində kompüterin, kontaktın, qrupun və ya istifadəçinin dəyişdirilməsi;
• **dsmove** – seçilmiş obyekti Active Directory xidmətinin digər yerinə köçürür və obyekti Active Directory xidmətinin ağacında yerini dəyişmədən adını dəyişdirir;
• **dsquery** – Active Directory xidmətində verilmiş sorğunun meyarları əsasında kompüteri, qrupu, serveri və ya istifadəçini axtarmağa imkan verir;
• **dsrm** – Active Directory xidmətində verilmiş tipdə olan obyekti və ya ixtiyari obyekti pozmağa imkan verir;
• **eventcreate** – sistem jurnalında administratora hadisə əlavə etmək imkanını verir;
• **eventquery** – bir və ya bir neçə sistem jurnalından hadisələri və onların parametrlərini təyin edir;
• **eventtriggers** – lokal və ya məsafədə olan kompüterdə hadisə trigerlərini təyin və konfiqurasiya edir;
• **forfiles** – paket emalı üçün kataloqdan faylları seçmək imkanını verir;
• **freedisk** – faylların quraşdırılmasından əvvəl diskdə boş yerin olması haqqında məlumat almağa imkan verir;
• **fsutil** – yönəltmə nöqtələrini "reparse point" idarə etmək və disk tomunun genişlənməsi imkanını verir;
• **getmac** – MAC-ünvan (Media Access Control) haqqında məlumatı və şəbəkə protokollarının siyahısını ekrana çıxarmaq imkanını verir;
• **gettype** – əməliyyat sistemi haqqında olan məlumata uyğun dəyişən sistem mühiti *%ERRORLEVEL%* təyin etmək imkanını verir;
• **gpresult** – həm qrup siyasətinin parametrlərini və həm də kompüterlər və ya istifadəçilər üçün qrup siyasətinin tətbiqi

nəticələrini təyin etməyə imkan verir;
• **helpctr** – "Help and Support Center" xidmətini işə salır;
• **inuse** – əməliyyat sisteminin kilidli faylarını əvəz edir;
• **iisback** – lokal və ya məsafədə olan kompüter üçün IIS xidmətinin konfiqurasiyasının ehtiyat surətlərini idarə etmək və yaratmaq imkanını verir;
• **iiscnfg** – lokal və ya məsafədə yerləşən kompüterdə IIS (Internet Information Services) konfiqurasiyasının hamısını və ya bir hissəsini idxal/ixrac edir;
• **iisftp** – IIS vasitəsinin 6.0-cı versiyası idarəçiliyi altında işləyən serverlərdə FTP-saytlarının siyahısını həm yaradır, həm də silir. Bundan başqa FTP-saytların işini dayandırmaq və yenidən işə salmaq kimi funksiyaları da özündə cəmləşdirir;
• **iisftpdr** – IIS vasitəsinin yeni versiyalarının idarəçiliyi altında işləyən serverlərdə FTP-saytlarının virtual kataloqlarını yaratmaq və silmək imkanına malikdir;
• **iisvdir** – IIS vasitəsinin yeni versiyalarının idarəçiliyi altında işləyən serverlərdə veb-saytların virtual kataloqlarını yaratmaq və silmək imkanına malikdir;
• **iisweb** – IIS vasitəsinin yeni versiyalarının idarəçiliyi altında işləyən serverlərdə veb-saytların siyahısını yaradır, göstərir və pozur. Bundan başqa işi dayandırmaq və yenidən işə salmaq kimi funksiyaları da özündə cəmləşdirir;
• **logman** – lokal və ya məsafədə yerləşdirilmiş kompüterdə "trace" əməliyyatının hadisələr jurnalının və istehsal qabiliyyətini əks elətdirən sayğaclardan verilənlərin yığılmasını planlaşdırmağa və idarə etməyə imkan verir;
• **nib** – "wlbs.exe" faylını şəbəkənin yüklənməsinin paylaşdırılması vasitələrini sazlamaq və idarə etmək üçün dəyişdirir;
• **nlbmgr** – bir kompüterdən klaster serverlərinin hamısını və yüklənmənin paylaşdırılması klasterinin konfiqurasiya və idarə etmək imkanına malikdir;

• **openfiles** – açıq fayllar haqqında məlumatı ekrana verir və onları bağlamaq imkanına malikdir;
• **pagefileconfig** – virtual yaddaş səhifələrinin sistem faylının parametrlərini sazlamaq və nəzərdən keçirmək funksiyasını yerinə yetirir;
• **perfmon** – "Performance Monitor" parametrləri fayllarının köməyi ilə sazlanan məhsuldarlıq konsolunu açmağa imkan verir;
• **prncnfg** – printer haqqında məlumatı konfiqurasiya etmək imkanını verir;
• **prndrvr** – lokal və ya məsafədə olan serverə qoşulan printerin drayverlərinin siyahısını hazırlamaq, əlavə etmək və silmək kimi əməliyyatları həyata keçirmək imkanını verir;
• **prnjobs** – çapda olan tapşırıqların siyahısını dayandırmaq, yenidən işə salmaq, ləğv etmək və hazırlamaq kimi əməliyyatları həyata keçirmək imkanını verir;
• **prnmngr** – lokal və ya qoşulmuş şəbəkə printerlərinin siyahısını hazırlamaq, əlavə etmək və silmək kimi əməliyyatları həyata keçirmək imkanını verir. Həmçinin ixtiyari printeri susma prinsipinə görə printer kimi təyin etmək və onun haqqında məlumatı ekrana çıxarmaq imkanını verir;
• **prnport** – çap serverinin TCP/IP standart portlarının siyahısını hazırlamaq, əlavə etmək və silmək, həmçinin onların konfiqurasiyalarını dəyişmək kimi əməliyyatları həyata keçirmək imkanını verir;
• **prnqctl** – printerin test səhifəsini çap etməklə yanaşı, printerin işini dayandırıb və ya yenidən işə salmaq və çap növbəsini tənzimləmək kimi əməliyyatları həyata keçirmək imkanını verir;
• **relog** – məhsuldarlıq jurnallarından məhsuldarlıq sayğaclarının göstəricilərini götürüb digər formata, yəni cədvəl şəkilli mətnlərə, ikili və ya SQL mətnlərinə keçirir.
• **rss** – disk fəzasını genişləndirmək üçün "Remote Storage" xidmətini aktivləşdirir;

• **sc** – xidmətlər parametrini qəbul edir və quraşdırır. Xidməti proqramları sınaqdan keçirir və sistemə uyğunlaşdırır;
• **schtasks** – verilmiş zaman kəsiyində və ya periodik olaraq proqramların yerinə yetirilməsini planlaşdırır. Cədvələ tapşırıqları əlavə edir və ya silir, tapşırıqları tələb yaranan kimi işə salır və ya dayandırır, həmçinin cədvələ baxışı və bu cədvəldə göstərilmiş tapşırıqların parametrlərinin dəyişdirilməsini təşkil edir;
• **setx** – heç bir proqramlaşdırma və ya ssenari yazılmasını tələb etmədən, lokal və ya sistemin dəyişkənlik mühitlərini təyin edir;
• **shutdown** – lokal və məsafədə olan kompüterin dayandırılması və ya yenidən işə salınması kimi əməliyyatları həyata keçirmək imkanı verir;
• **systeminfo** – kompüterin konfiqurasiyası haqqında baza məlumatlarını əldə etmək imkanını verir;
• **takeown** – administratora, fayla olan girişi bərpa etməyə imkan yaradır;
• **taskkill** – bir və ya bir neçə tapşırıqların və proseslərin bitirilməsinə imkan yaradır.
• **tasklist** – lokal və ya məsafədə olan kompüterdə hal-hazırda yerinə yetirilən sistem proqramların, xidmətlərin, proseslərin identifikatorlarının siyahısını tərtib edir;
• **timeout** – komanda prosesinin işini müəyyən olunmuş müddətə dayandırır;
• **tracerpt** – xüsusi aparat qurğularından real zaman rejimində alınmış "trace" əməliyyatının hadisələr jurnalını emal edir, "trace" əməliyyatının analiz hesabatlarını və CSV fayllarını generasiya etməyə imkan verir;
• **tsecimp** – informasiyanı XML faylından serverin mühafizə faylı olan TAPI (tsec.ini) faylına idxal edir;
• **typeperf** – məhsuldarlıq sayğacının göstəricilərini komanda sətri pəncərəsinə və ya dəstəklənən formatın jurnalının faylına çıxarır;
• **waitfor** – şəbəkədə olan bir neçə kompüteri sinxronlaşdırmaq üçün siqnallardan istifadə edir;

• **where** – müəyyən olunmuş parametrə uyğun gələn bütün faylları tapıb çıxarır;
• **whoami** – sistemə daxil olarkən qeydə alınan domenin və ya kompüterin adı, istifadəçinin adı, qrupun adı, istifadəçinin identifikatoru və cari istifadəçinin üstünlüklərini geri qaytarır;
• **WMIC** – (WMI Command line) komanda sətrinin əmri, komanda sətri servisi üçün sadə sayılan əmrlərdəndir. WMIC əmri – Windows əməliyyat sistemi olan kompüterləri idarə etmək üçün istifadə olunur və komanda sətrinin digər əmrləri ilə tam uyuşur. WMI əmri vasitəsi ilə idarə olunan kompüterlərin istifadəsi asanlaşır.

5.10 İstifadəçilərin miqrasiyası

Böyük həcmli şirkətlərdə USMT (User State Migration Tool – İsitfadəçilərin Miqrasiya Aləti) vasitəsi korporativ şəbəkənin çox sayda olan istifadəçilərinin fayl və parametrlərinin miqrasiya prosesini sadələşdirir. USMT vasitəsi lazımi parametrləri sazlamağa geniş imkanlar yaradır, məsələn, reyestri komanda sətrinin əmrlərinə məxsus dəqiqliklə sazlamağa imkan verir. USMT vasitəsi ancaq korporativ şəbəkənin administratorları üçün nəzərdə tutulub. USMT vasitəsinin işləməsi üçün korporativ şəbəkənin işçi stansiyası hökmən MS Windows Server 2003 əməliyyat sistemi domen kontrollerinə qoşulmalıdır.
USMT vasitəsi aşağıda sadalanan istiqamətlərdə yaxşılaşma vəd edir:
• texniki mütəxəssislərə yönələn xərclərin azalması;
• mütəxəssislər tərəfindən əməliyyat sisteminin istifadəçi interfeysinin sazlanmasına itirilən vaxtın azaldılması;
• işçilərin itirilmiş faylların və qovluqların axtarılmasına sərf etdiyi zamanın azaldılması;
• əməliyyat sisteminin istifadəçi interfeysinin sazlanması üçün işçilərin texniki bölməyə müraciətlərinin azaldılması;

• yeni əməliyyat sisteminin istifadəçilər tərəfindən başa düşülməsinə sərf etdiyi zamanın azaldılması;
• miqrasiyadan sonra istifadəçilərin tələblərinin qarşılanması;

USMT vasitəsi iki icraçı fayldan və miqrasiya haqqında məlumatı özündə cəmləyən dörd fayldan ibarətdir. Bu icraçı fayllar "ScanState.exe" və "LoadState.exe"-dir. Miqrasiya haqqında məlumatı özündə cəmləyən dörd fayllar bunlardır: Migapp.inf, Migsys.inf, Miguser.inf və Sysfiles.inf.
"ScanState.exe" faylı istifadəçi verilənlərinin və parametrlərinin Migapp.inf, Migsys.inf, Miguser.inf və Sysfiles.inf fayllarında olan informasiya əsasında yığımını təşkil edir. Toplanılmış verilənləri "LoadState.exe" faylı, korporativ şəbəkənin yeni yazılmış MS Windows XP Professional əməliyyat sistemi olan kompüterinə yerləşdirir. USMT vasitəsi «.inf» fayları yığımı idarəçiliyi altında işləyir. Onlar korporativ şəbəkənin administratoru tərəfindən və ya avadanlıq istehsal edən müstəqil istehsalçılar tərəfindən yeniləşdirilə bilərlər. USMT vasitəsini istifadə edən zaman miqrasiyanı avtomatlaşdırmaq üçün administrator tərəfindən, hökmən mövcud «.inf» fayllarının adını dəyişdirmək lazımdır. Bu əməliyyatı etdikdən sonra yeni «.inf»" faylları müvafiq hesablama mühitinə daha uyğun olacaqlar. Miqrasiyanın əlavə qaydalarını izah etmək üçün yeni «.inf» fayllarının yaradılması praktik cəhətdən məqsədəuyğun olardı. Parametrlərə heç bir dəyişiklik etmədən USMT vasitəsi susma prinsipinə görə aşağıdakı komponentləri miqrasiya edir:
• Outlook Express parametrləri və yaddaş qovluqları;
• MS Outlook parametrləri və yaddaş qovluqları;
• Internet Explorer parametrləri;
• telefoniya və modemlərin parametrləri;
• Office proqram paketinin standart fayl tiplərini;
• məhdud fiziki imkanlara malik, fiziki şəxslər üçün parametrlər;
• klassik «İş masası»;
• ekran qoruyucusunun seçilməsi;

- asinxron kommunikasiya parametrləri;
- qovluqların parametrləri;
- «Desktop» qovluğunu;
- «My Documents» qovluğunu;
- «My Pictures» qovluğunu;
- «Favorits» qovluğunu;
- «Cookies» qovluğunu;
- idarəetmə panelinin parametrləri;
- klaviatura və manipulyasiya qurğularının parametrləri;
- Office proqram paketinin parametrləri;
- şəbəkə printerləri və diskləri.

Toplanan məlumatı **ScanState.exe** proqramı vasitəsi ilə asanlıqla modifikasiya etmək mümkündür. Bu sistem proqramını əks prinsiplə işləməyə sazlamaq olar, yəni faylları, qovluqları reyestrin yazılarını və bölmələrini nəzərə almasın.

5.11 Windows Installer

"Windows Installer" vasitəsi quraşdırılma parametrlərinin sazlanması, yeniləşməsi, təzə proqramların yazılması prosesini sadələşdirməyə imkan verir və konfiqurasiya ilə bağlı bir sıra problemləri həll edir. "Windows Installer" ümumi resursları idarə edir, faylların versiyalarının yoxlanılmasında, əvvəlcədən razılaşdırılmış qaydaların tətbiq olunmasına təminat verir və həmçinin sistem proqramların iş zamanı onların diaqnostikasını və bərpasını həyata keçirir, bu da öz növbəsində sistem proqramların idarə olunmasında hərtərəfli qənaətə səbəb olur. "Windows Installer" vasitəsi yeni proqram təminatının yazılması üçün müxtəlif texnologiyalar tətbiq edir. Hər bir proqram təminatı üçün unikal quraşdırılma qaydalar yığımına malikdir. Bəzən proqram təminatını korporativ şəbəkənin hər hansı bir işçi stansiyasına yazdıqda bir sıra problemlər mövcud olur. Misal kimi faylın köhnə versiyasının artıq sistemdə mövcud olan eyni faylın yenisinin üzərinə səhvən yazılması halını göstərmək olar.

Proqramların quraşdırılma prosesində çox sayda texnologiyaların tətbiq olunması bir kompüterdə eyni zamanda müxtəlif sistem proqramlar tərəfindən birgə istifadə olunan komponentlərə olan müraciətlərin sayının təyin olunmasını çətinləşdirir. Nəticədə bir proqramın pozulması və ya yenidən kompüterə yazılması zamanı korporativ şəbəkənin digər istifadəçilərinə mane ola bilər. "Windows Installer" vasitəsinin istifadəsi zamanı proqramın yüklənməsinin bütün qaydaları əməliyyat sistemi tərəfindən müəyyən edilir. Bütün bu deyilən problemlərlə üzləşməmək və qaydalara tam riayət etmək üçün sistem proqramını "Windows Installer" paketinə tanıtmaq kifayətdir. Sonra isə hər bir sistem proqramın quraşdırılması "Windows Installer" vasitəsi ilə yerinə yetirilir. Beləliklə quraşdırılma zamanı olan problemlərin korporativ şəbəkədə yayılmasının qarşısı alınmış və ya minimuma endirilmiş olacaqdır.

MS Windows Server 2003 əməliyyat sistemi yeni imkanlar təklif edir. Bu imkanlar vasitəsi ilə informasiya təhlükəsizliyinin qorunması daha yüksək səviyyədə olur və həmçinin "Windows Installer" vasitəsinin istifadəsini və idarə edilməsini rahatlaşdırır.

64-bitlik dəstək. Windows Installer vasitəsi, MS Windows Server 2003 əməliyyat sisteminin "Enterprise Edition" və "Datacenter Edition" buraxılışlarının 64-bitlik versiyalarında əsil 64-bitlik xidmət kimi realizə olunmuşdur.

"Windows Installer" vasitəsi həm 32, həm də 64-bitlik sistem proqramların quraşdırılmasını yerinə yetirir. 64-bitlik sistem proqramlar xüsusi vasitə ilə ayrılmış 64-bitlik "Windows Installer" paketinə yerləşdirilirlər. Lakin burada həm 32, həm də 64-bitlik komponentlərin quraşdırılması mümkündür.

Proqram təminatının istifadəsini məhdudlaşdıran siyasət. Proqram təminatının istifadəsini məhdudlaşdıran siyasətin korporativ şəbəkədə tətbiq olunması, şəbəkəni şübhəli proqram təminatından qorumağa şərait yaradır. Bu siyasətin üstünlüyü

ondan ibarətdir ki, yalnız əvvəlcədən təyin olunmuş proqram vasitələri işçi stansiyaya yazıla bilər. Proqram təminatlarının identifikasiya olunması üçün sistem heş-qaydalardan, sertifikat qaydalarından, İnternet zonalarından istifadə edir. "Windows Installer" vasitələrinin paketləri və transformasiyaları proqram təminatının istifadəsini məhdudlaşdıran siyasətin qaydalarına tabe olurlar. İstifadəçilər tərəfindən hər hansı bir proqramın işə salınması üçün iki səviyyə mövcuddur, bunlardan birincisi: məhdudiyyətsiz və ikincisi: məhdudiyyətli. Adətən "Windows Installer" vasitəsi, ancaq səviyyə göstəricisi məhdudiyyətsiz olan paketləri realizə edir. Əgər quraşdırılma prosesində transformasiya elementləri aktivdirsə, onda quraşdırılmanı uğurla başa çatdırmaq üçün onlara səviyyə göstəricisi məhdudiyyətsiz təyin olunmalıdır. Əgər proqram təminatının istifadəsini məhdudlaşdıran siyasətin qaydalarına əsasən proqram paketinin səviyyə göstəricisinə məhdudiyyətli parametr təyin olunubsa, bu zaman "Windows Installer" vasitəsi baş vermiş səhv haqqında məlumatı ekrana çıxaracaq. Belə olan halda dərhal hadisələr jurnalında bu səhvi əks etdirən sistem yazısı yerləşdirilir. Əməliyyat sistemi proqram təminatının istifadəsini məhdudlaşdıran siyasətin qaydalarını, proqram vasitəsinin işçi stansiyaya ilk dəfə quraşdırılan zaman tətbiq etməyə başlayır. Eyni tətbiqetmə əməliyyatını "Windows Installer" vasitəsi keşdə proqramın quraşdırılma paketini bərpa etmək lazım olduqda yerinə yetirir. Korporativ şəbəkənin sistem administratoru və digər istifadəçilər üçün proqram təminatının istifadəsini məhdudlaşdıran qaydaları müxtəlif "Windows Installer" paketlərinə tətbiq etmək mümkündür.

5.12 Korporativ şəbəkələrin məsafədən idarə olunmasının əsas elementləri

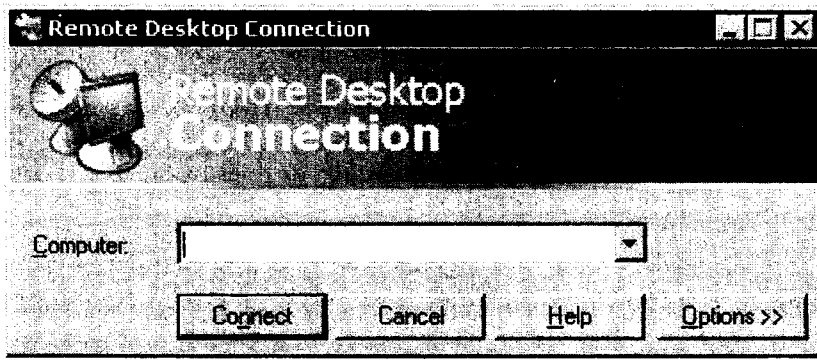
MS Windows Server 2003 əməliyyat sistemi əlavə olaraq məsafədən idarəetmə imkanlarını özündə cəmləşdirir. Bunlradan

"Remote Desktop for Administration" – "Terminal Services" hissəsi, "Microsoft Management Console" (MMC), "Active Directory Services Interface" (ADSI), "Telnet" xidmətləri və "WMI" alətini göstərmək olar. Sadalanan vasitələri iki böyük qrupa ayırmaq olar: MS Windows Server 2003 əməliyyat sisteminin daxilində olan vasitələr, məsələn: Active Directory, qrup siyasəti, hadisələr dispetçeri, xidmətlər və s.; ikinci qrupa isə korporativ şəbəkələrin kompüterlərinə "Remote Desktop" təminatı vasitəsi ilə məsafədən qoşulmanı aid etmək olar. MS Windows Server 2003 əməliyyat sistemi olan serverlər müxtəlif mühafizəlilik dərəcəsi olan korporativ şəbəkələrdə işləməyə qadirdirlər. Belə mühitdə korporativ şəbəkənin serverləri lokal əməliyyat etmədən məsafədən tam şəkildə idarə oluna bilər, yəni serverdə heç bir əlavə qoşulan qurğulardan (klaviatura, monitor, video kart və s.) istifadə etmədən. Korporativ şəbəkənin administratoru bir nöqtədən bir neçə serveri eyni zamanda diaqnostika edib, müxtəlif tip problemləri uzaqlaşdıra və tam şəkildə idarə edə bilər. Lakin məsafədən idarəetmədə mümkün olmayan funksiyalar da mövcuddur, bunlardan serverə avadanlığın qoşulması və ya dəyişdirilməsini göstərmək olar. Avadanlığın qoşulması və ya dəyişdirilməsi əməliyyatından başqa ixtiyari nöqtədən korporativ şəbəkənin serverinin məsafədən idarə etmək mümkündür.

İdarəetmə vasitələrinin düzülüşü. Proqram təminatının müstəqil istehsalçıları həddindən çox sayda korporativ şəbəkələri məsafədən idarəetmə vasitələrini təklif edirlər. Belə halda hadisələrin idarəetmə aləti, bir neçə sistemdə külli miqdarda hadisələrin toplanmasından daha çox yararlı ola bilər. Digər alətlər içində isə – genişlənməni nəzərə alan və işləmə qabiliyyətinin monitorinq vasitəsi olan alətləri qeyd etmək olar. Genişlənməni nəzərdə tutan alətin funksiyası, korporativ şəbəkənin administratorunu yeni əlavə qurğuların quraşdırılması haqqında təlimatlandırmaq üçündür. İşləmə qabiliyyətinin

monitorinq alətinin əsas funksiyası isə təhlükəsizlik vasitələrinin müntəzəm şəkildə monitorinq etməkdən ibarətdir.

Remote Desktop. Remote Desktop (Remote Desktop for Administration) köhnə versiyalarda "Remote Administration" rejiminin "Terminal Services" funksiyası kimi tanınırdı (şəkil 5.10). "Remote Desktop" vasitəsi korporativ şəbəkənin MS Windows Server 2003 əməliyyat sistemi quraşdırılmış ixtiyari serverinin "iş masasına" məsafədən girişi təmin edir. Bu funksiya korporativ şəbəkənin serverini həmin şəbəkəyə məxsus ixtiyari işçi stansiyasından idarəetməyə imkan verir.



Şəkil 5.10 Remote Desktop Connection pəncərəsi

Serverlərin "Remote Desktop for Administration" vasitəsinin köməyi ilə məsafədən idarə edilməsini korporativ şəbəkənin MS Windows Server 2003 əməliyyat sistemləri ailəsinə məxsus ixtiyari versiyalı kompüterindən həyata keçirmək olar. MS Windows XP əməliyyat sistemində bu vasitənin sadələşdirilmiş variantı olan "Remote Desktop" realizə olunmuşdur. "Remote Desktop for Administration" vasitəsi korporativ şəbəkənin idarə edilməsi xərclərini hiss oluna biləcək dərəcədə aşağı sala bilər. "Terminal Services" texnologiyası əsasında quraşdırılan "Remote Desktop for Administration" vasitəsi məhz korporativ şəbəkələrin serverlərini idarə etmək üçün nəzərdə tutulub. "Terminal Server"

komponentləri tərəfindən realizə olunmuş bəzi sistem proqramlarının birgə istifadə olunmasını, çoxistifadəçilik imkanlarını və proseslərin cədvəl üzrə yerinə yetirilməsi funksiyalarını dəstəkləmir. Nəticə etibarı ilə prosessorun yükünü artırmadan "Remote Desktop for Administration" vasitəsini həddindən artıq yüklənmiş serverə tətbiq etmək məqsədə uyğundur. Məhz bu səbəbdən "Remote Desktop for Administration" vasitəsi korporativ şəbəkələrin serverlərinin məsafədən idarə edilməsində çox rahat və effektiv servis kimi tətbiq oluna bilər. "Remote Desktop for Administration" vasitəsi korporativ şəbəkənin işçi stansiyaları üçün əlavə lisenziyaların alınmasını tələb etmir və "Terminal Server Licensing" sistem proqramının quraşdırılmasına da heç bir lüzum qalmır. Windows əməliyyat sisteminin köhnə versiyaları olan korporativ şəbəkənin kompüterlərinə "Remote Desktop Connection" vasitəsini yazaraq, MS Windows Server 2003 əməliyyat sistemi üçün ixtiyari növ idarəetməni tətbiq etmək mümkündür.

5.13 Korporativ şəbəkənin təhlükəsizlik siyasətinin idarə olunmasının avtomatlaşdırılması

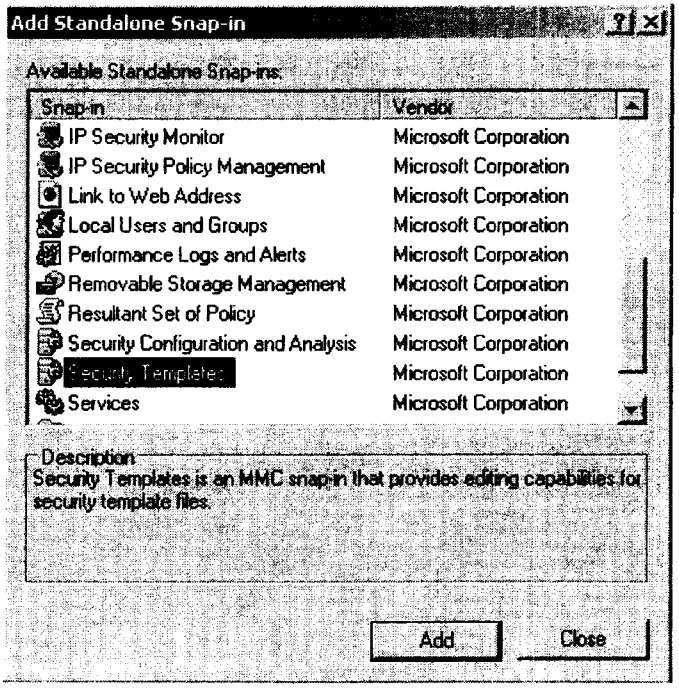
Fayl sistemləri və qeydiyyat yazıları ilə işi nəzərdən keçirərək administratorun işinin asanlaşdırılması və əməliyyat sisteminin işləmə qabiliyyətinin artırılması əsas şərtlərdən biridir. Əgər çox sayda kompüterə malik korporativ şəbəkəni qurmaq tələb olunursa, onda təhlükəsizlik siyasətinin idarə olunmasını sadələşdirmək mümkündür. Əgər dəyişdiriləcək parametrlərin sayı həddindən çoxdursa və korporativ şəbəkəni kompüterləri bir-birindən uzaq məsafədə yerləşirsə, onda təhlükəsizlik şablonları komanda sətri vasitəsi ilə və ya məsafədə olan kompüterin idarəetmə konsolu vasitəsi ilə idarı olunur.

C:\WINDOWS\system32 qovluğunda "msc" genişlənməsi ilə olan fayllar yerləşirlər. Bu bir çox obyektlərin, kompüterin xidmətləri və domenin idarəetmə konsolunun fayllarıdır.

Menyudan lokal təhlükəsizlik parametrlərinə uyğun olan bənd seçildikdə, məsələn:
"mmc.exe" proqramı **C:\WINDOWS\system32\secpol.msc** faylını açmış olacaq. Digər tərəfdən "mmc.exe" proqramı standart əməliyyat vasitəsi ilə açıla bilər, **Start→Run→mmc**. Açılan proqramda kompüteri idarə etmək üçün müxtəlif variantlar daxil etmək mümkündür. Hər hansı bir təchizat qaydasını daxil etmək üçün yuxarı menyuda **Console → Add/Remove Snapp-in...→Add** bəndini seçmək tələb olunur.

Açılmış "Add standalone Snapp-in" pəncərəsində (şəkil 5.11) lazımi təchizat qaydasını seçmək mümkündür. Seçdikdən sonra yuxarı menyuda **Console→Save as...** bəndini seçirik. Burada konsol faylını ixtiyarı parametrlərlə və müxtəlif təchizat qaydalarına tənzimlənmiş şəkildə yadda saxlamaq mümkündür. Əlavə etmək mümkün olan təchizat qaydaları içərisində "Security Configuration and Analysis" bəndi də mövcuddur. Bu təchizat qaydası vasitəsi ilə cari təhlükəsizlik parametrlərinin analizini keçirmək olar. Bunun üçün verilənlər bazasının faylını seçmək və cari təhlükəsizlik parametrlərini şablon faylında saxlamaq kifayətdir. Kompüterin cari təhlükəsizliyini idxal etdiyimiz təhlükəsizlik şablonuna
əsasən dəyişdirə bilərik.

Bunun üçün yuxarı menyudan **Action→Import Tempalte** bəndini seçmək lazımdır. Əməliyyat sisteminin distributiv versiyasından və sistemə olunan yeniləşmələrdən asılı olaraq "Import Tempalte" bəndi, "Import Policy" bəndi ilə əvəz oluna bilər. Analiz keçirilən zaman vahid bir "log" fayl yaradılacaq. Bu faylın içində əməliyyat sistemi baxımından təhlükəsizlik parametrlərində bütün boşluqlar sadalanılacaq. Alınmış konsola lazım olan bəzi qaydaları əlavə edərək, onu gələcəkdə istifadə etmək məqsədi ilə yadda saxlamaq olaq. Burada daha bir maraqlı qaydaya fikir vermək pis olmazdı. Məsələn, təhlükəsizlik şablonları (Security Templates).



Şəkil 5.11 İzolə etmə təchizatının əlavə olunması pəncərəsi

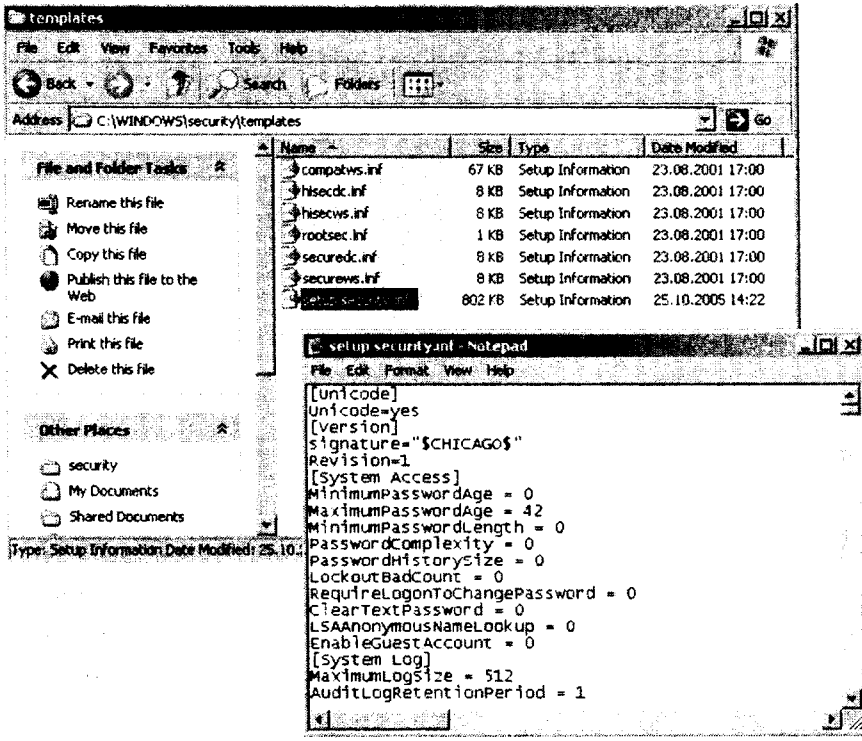
Bu təchizat vasitəsi ilə yeni təhlükəsizlik şablonlarını yaratmaq mümkündür. Müvafiq qaydaları korporativ şəbəkənin bir və ya bir neçə kompüterinin konfiqurasiyasını dəyişdirmək üçün istifadə etmək olar. Bu kompüterlərin konfiqurasiyalarının dəyişdirilməsi komanda sətrindən işə salınan "Secedit.exe" proqramının "Security Configuration and Analysis" təchizatı və ya "Local Security Settings" təchizatına müvafiq şablonun yüklənməsi vasitəsi ilə həyata keçirilə bilər. Təhlükəsizlik şablonları standart olaraq aşağıda göstərilən ünvanda yerləşirlər:

C:\WINDOWS \Security\Templates.

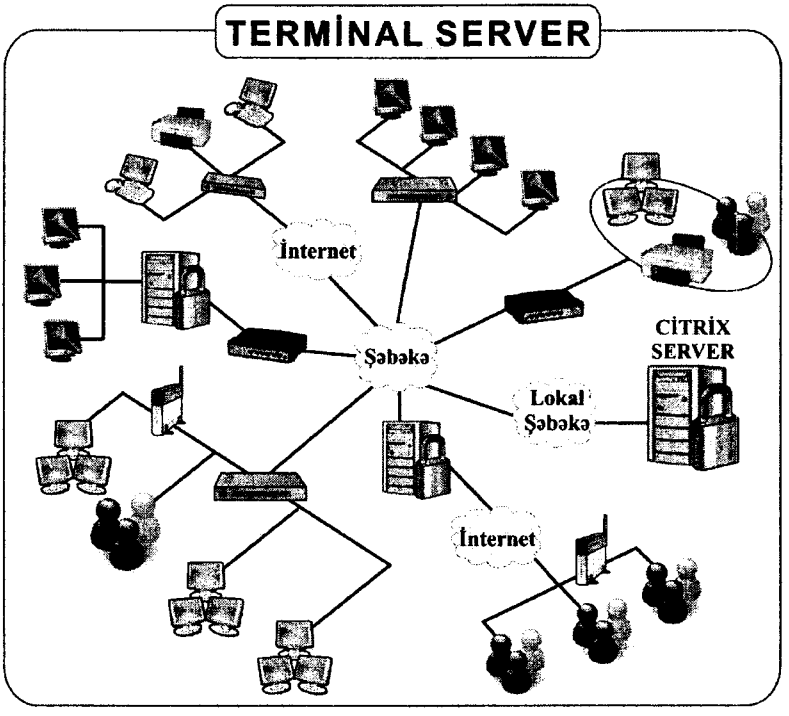
Əməliyyat sistemini quraşdırdıqdan sonra sistemdə aşağıdakı şablonların olması mümkündür:

• **Setup security.inf** – əməliyyat sisteminin quraşdırılması zamanı tətbiq olunan təhlükəsizlik parametrlərini və sistem diskin əsas kataloqunun fayllarının icazələrini özündə cəmləyir (şəkil 5.12). Bu şablondan sistemin çökməsindən sonra bərpa etmədə istifadə etmək olar.

• **Compatws.inf** – domen kontrollerləri olmayan işçi stansiyalar və serverlər üçün standart icazələri özündə cəmləyir. Lokal qrupun daxili strukturu və iyerarxiyası nəzərə alınır, yəni "Administrator", "Təcrübəli İstifadəçilər", "İstifadəçilər".



Şəkil 5.11 "Setup security.inf" təhlükəsizlik şablonu



FƏSİL 6

TERMİNAL SERVER

TERMİNAL SERVER

- Terminal serverin rolunun təyin olunması
- Terminal serverin sazlanması
- İcazələrin uyğunlaşması
- Lisenziyalaşdırma
- Qrup siyasətlərinin sazlanması

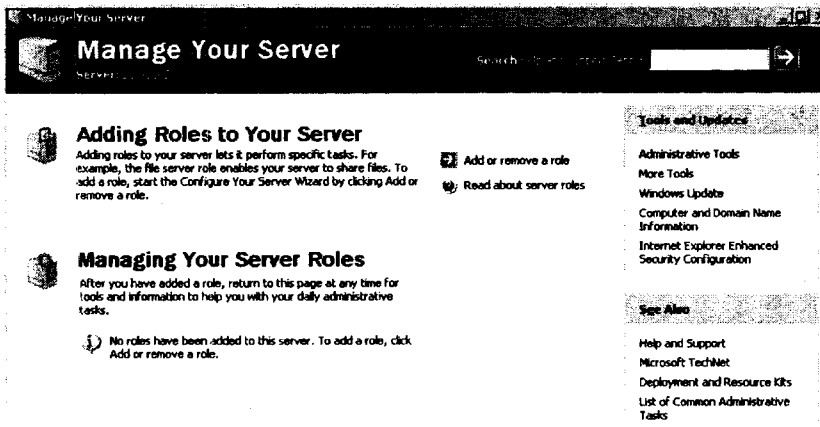
Fəsil 6. TERMİNAL SERVER

6.1 Terminal serverin rolunun təyin olunması

Terminal Server texnologiyasının əsas məqsədi ondan ibarətdir ki, bütün proqramlar istifadəçi kompüterində deyil, mərkəzi serverdə yerinə yetirilsin. Belə yanaşma zamanı aşağıdakı üstünlükləri qeyd etmək olar:

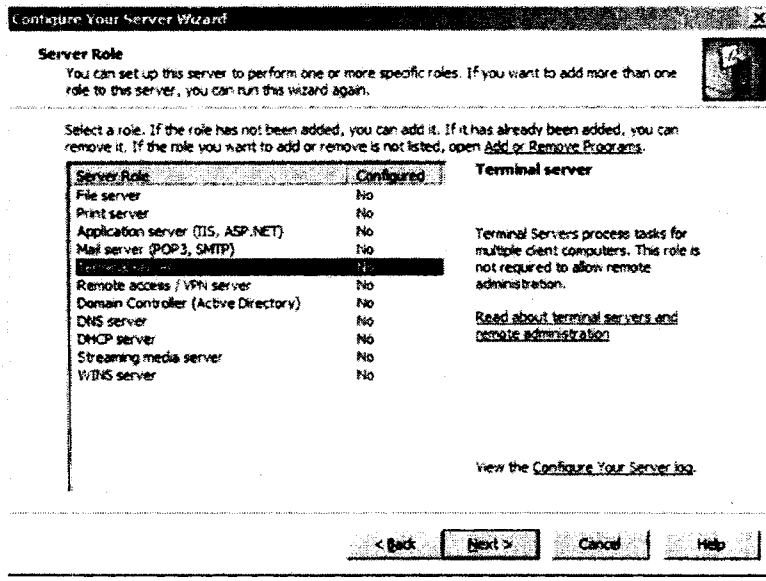
- Korporativ şəbəkədə məlumatların emalı artıq işçi stansiyasının gücündən asılı olmayacaq və belə olan halda istifadəçiləri çox da baha olmayan texniki təchizatla təmin etmək mümkündür;
- Məlumatların emalı korporativ şəbəkənin mərkəzi serverində baş verdiyindən, sistemi elə sazlamaq olar ki, bədəməl şəxs şəbəkə daxili məlumatları hər hansı bir nəzərdə tutulmayan variantda ələ keçirə bilməsin. Məsələn, verilənlər bazasının əsas fayllarını korporativ şəbəkəyə məxsus olmayan digər kompüterlərdə açılmasının qeyri-mümkünlüyü;
- Korporativ şəbəkədə məlumatların emalı birbaşa olaraq mərkəzi serverdən asılı olduğundan sistemin məhsuldarlığının artırılması üçün yalnız serveri yeniləşdirmək kifayət edir. Bu isə öz növbəsində maliyyə baxımından təşkilatlar üçün bir neçə fərdi kompüteri yeniləşdirməkdən daha sərfəlidir;
- Terminal server texnologiyası digər şəbəkə texnologiyaları ilə müqayisədə, korporativ şəbəkələrin texniki parametrlərinə və məhsuldarlığına az tələblər irəli sürür. Belə olan halda isə terminal rejimdə kiçik sürətli şəbəkə bağlantıları və İnternet şəbəkəsi vasitəsi ilə işləmək mümkün olur.

Korporativ şəbəkənin administratoru MS Windows Server 2003 əməliyyat sistemini quraşdırdıqdan sonra, serverə ilk girişi zamanı ekranda "Manage Your Server" pəncərəsi (şəkil 6.1) açılır.



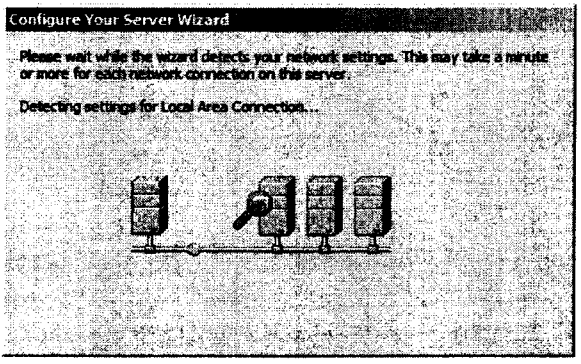
Şəkil 6.1 MS Windows Server 2003 əməliyyat sistemində "Manage Your Server" pəncərəsi

"Configure Your Server" vasitəsinin işini başlatmaq üçün "Add or remove a role" bəndini seçmək lazımdır. Bu bəndi seçdikdən sonra növbəti pəncərə (bax şəkil 6.2) açılır.



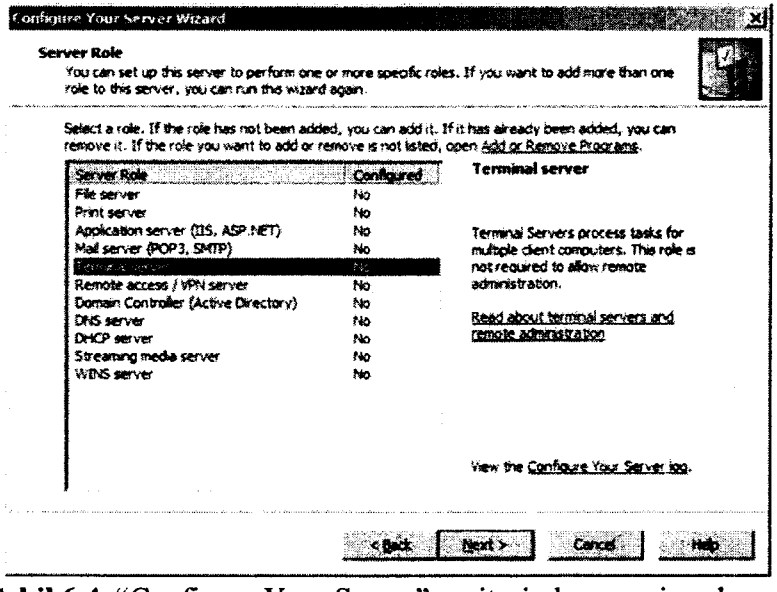
Şəkil 6.2 "Configure Your Server Wizard" pəncərəsi

Sonra quraşdırılma vasitəsi korporativ şəbəkə daxilində bütün bağlantıları yoxlamağa başlayır (şəkil 6.3). Bu yoxlanış uyuşan rolları müəyyən etmək və mümkün olan rolların təyin olunması məqsədi ilə aparılır.



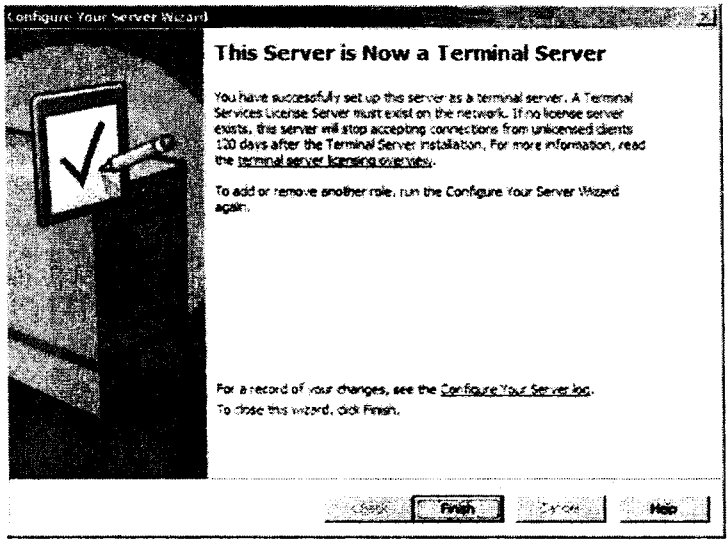
Şəkil 6.3 Bağlantıların yoxlanışı pəncərəsi

Axtarış əməliyyatından sonra tələb olunan rolu, məsələn terminal serveri seçib "Next" düyməsinə basırıq (bax şəkil 6.4).



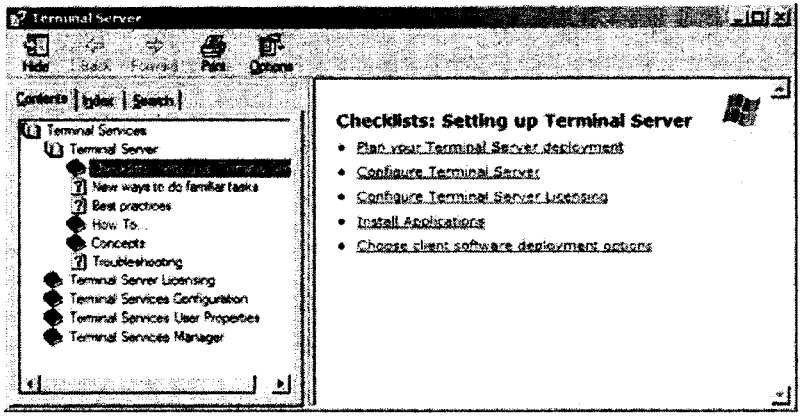
Şəkil 6.4 "Configure Your Server" vasitəsində serverin rolunun seçilməsi

Quraşdırılma vasitəsi əməliyyat sisteminin yenidən işə salınması haqqında ekrana bildiriş çıxaracaq və bu əməliyyatdan sonra "Add/Remove Windows Components" appleti yeni rol üçün tələb olunan xidmətlər toplusunu işə salmaq məqsədi ilə yerinə yetiriləcək. Bu xidmətlər quraşdırıldıqdan sonra server yenidən işə salınır. Rolun əlavə olunması zamanı kompüterin yenidən işə salınması əməliyyatı məcburidir və bunu daha sonraya saxlamaq mümkün deyil. Kompüter yenidən işə salınan zaman, sistemdə qeydiyyatdan keçmək lazımdır. Qeydiyyat zamanı iki pəncərə açıq vəziyyətdə olur, bunlardan biri terminal serverin rolunun müvəffəqiyyətlə quraşdırıldığı haqqında məlumat verir (şəkil 6.5).



Şəkil 6.5 Terminal serverin müvəffəqiyyətlə quraşdırılmasının pəncərəsi

İkinci pəncərə isə (şəkil 6.6) özündə çox dəyərli məlumat daşıyır, bu quraşdırılma prosesini tam başa çatdırmaq üçün növbəti addımların siyahısıdır.



Şəkil 6.6 Terminal serveri sazlamaq üçün növbəti addımların siyahısı

6.2 Terminal serverin sazlanması

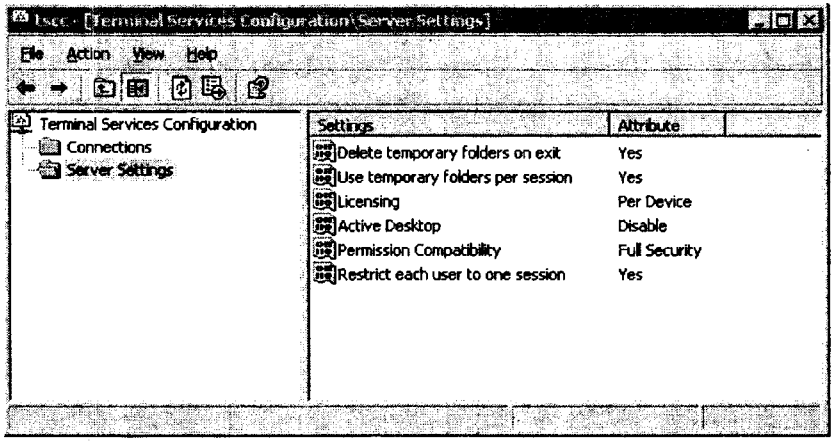
Şəkil 6.6-dan göründüyü kimi terminal server quraşdırıldıqdan sonra sazlanması üçün bir sıra addımlar atmaq lazımdır. Terminal serveri sazlamaq üçün bəzi lazımi məlumatlar "Plan your Terminal Server Deployment" bölməsində yerləşir. Terminal serverin konfiqurasiya edilməsinin iki əsas aləti mövcuddur. Bunlardan birincisi "Terminal Services Configuration" və ikincisi "qrup siyasətlərinin redaktorunu" göstərmək olar. " Terminal Services Configuration" sistem vasitəsi terminal serverin konfiqurasiya olunmasının əsas vasitəsidir. Bu sistem alətin köməyi ilə korporativ şəbəkənin administratoru server üçün səlahiyyət rejiminin təyin edilməsi, məhsuldarlıq göstəricilərinin sazlanması və RDP (Reliable Data Protocol) sazlanması kimi vacib elementləri quraşdırıb sazlaya bilər. "Terminal Services Configuration" vasitəsini üç cür işə salmaq olar:

1) "Start" menyusundan "Administrative Tools" bəndini seçərək;
2) "Configure Terminal Server" quraşdırılma vasitəsindən;
3) "Manage Your Server" idarəetmə vasitəsindən.

Şəkil 6.7-də "Server Settings" qovluğunda altı parametrin olduğunu görmək mümkündür.
Onlardan üçünü – "Delete temporary folders on exit", "Use temporary folders per session" və "Active Desktop" adətən susma prinsipinə görə sistem necə təyin edirsə, administratorlar da olduğu kimi saxlayırlar.

- "Delete temporary folders on exit" (çıxış zamanı müvəqqəti faylların silinməsi). Terminal serverdə hər bir istifadəçiyə müvəqqəti qovluq ayrılır. Bu qovluğun sistemdəki ünvanı aşağıdakı kimidir:

C:\Documents and Settings\<username>\local settings\temp.



Şəkil 6.7 "Terminal Services Confiquration" pəncərəsinin "Server Settings" qovluğu

Əgər bu vasitə aktivdirsə, onda istifadəçi sistemdən çıxdığı zaman bu qovluğun tərkibində olan fayllar silinəcək. Əgər korporativ şəbəkənin daxilində dəyişkən profillər istifadə olunursa və "Delete cached copies of roaming profiles" siyasəti qoşulubsa, onda "Delete temporary folders on exit" funksiyası öz mənasını itirir. Odur ki, bu funksiyanı aktiv şəkildə hər zaman saxlamaq məqsədə uyğundur, xüsusən köhnə seansdan müvəqqəti faylları tələb edən

proqramlar olmadığı hallarda. Bu halda administrator korporativ şəbəkənin qrup siyasətinə dəyişiklik etməlidir.

- "Use temporary folders per session" (hər bir seans üçün müvəqqəti qovluğun istifadəsi). Əgər bu funksiya aktivdirsə, onda istifadəçinin hər seansına yeni müvəqqəti qovluq yaradılır. Bu qovluqlar sistemdə

C:\Documents and Settings\<username>\local settings\temp0 və ya **temp1, temp2** və s. kimi işarələnir. Belə halda ayrı-ayrı seanslar bir-birinə mane olmurlar.

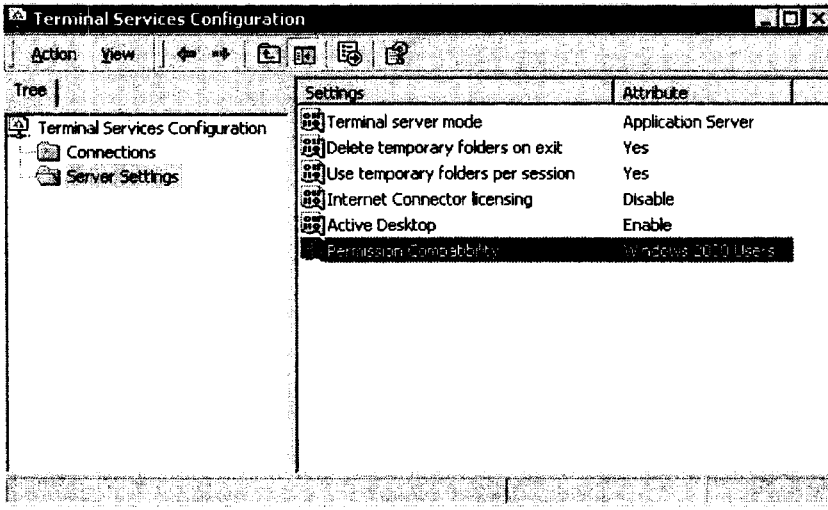
- "Active Desktop" – MS Windows 98 əməliyyat sistemindən başlayaraq, iş masasının üzərinə aktiv tərkibli elementlərin əlavə olunması mümkün olub. Aktiv tərkibli elementlər dedikdə – veb-səhifə, animasiya, xəbər başlıqları və bu kimi məlumatlar başa düşülür. Ekranın göstərmə qabiliyyətini və sistemin artıq dərəcədə yüklənməsini nəzərə alaraq terminal serverdən təyin olunan istifadəçilər üçün susma prinsipinə görə "Active Desktop" vasitəsi aktiv olmur.

"Server Settings" qovluğunun qalan digər üç parametri isə -"Licensing", "Permission Compatibility" və "Restrict each user to one session" – daha çox diqqət və zəhmət tələb edirlər. Bu parametrlər terminal serverdə quraşdırılmış əməliyyat sistemindən və proqramlardan birbaşa asılıdır.

6.3 İcazələrin uyğunlaşması (Permission Compatibility)

MS Windows Server 2003 əməliyyat sistemində "Terminal Services" xidmətlərini (şəkil 6.8) quraşdıran zaman sistem "icazələrin uyğunlaşması" rejimini seçməyi təklif edəcək. Uyğunlaşmağa təklif olunan variantlarda MS Windows 2000 Server və ya "Terminal Server 4.0" olacaq. MS Windows Server 2003 əməliyyat sistemində təhlükəsizlik anlayışına çox böyük yer ayrılmışdır, məhz bu səbəbdən əməliyyat sistemi susma prinsipinə görə serveri "Full Security" (tam təhlükəsizlik) rejiminə sazlayır.

"Tam təhlükəsizlik" rejimində işləyən serverdə korporativ şəbəkənin administratorundan fərqli olan, digər statuslu istifadəçilər **HKEY_LOCAL_MACHINE** reyestr açarını dəyişdirə bilməzlər və faylları öz profillərinə məxsus qovluqlardan başqa heç bir yerə yaza bilməzlər. Lakin praktikada belə hallarda mövcud olur ki, "tam təhlükəsizlik" rejimində bəzi proqramlar işləmir. Bu vəziyyətdən çıxış yolu kimi "Relaxed Security" (zəiflədilmiş təhlükəsizlik) rejiminə keçmək məqsədə uyğundur. Amma bu rejimi yalnız çıxış yolu olmayan hallarda tətbiq etmək lazımdır, çünki bu rejim korporativ şəbəkənin adi istifadəçiləri üçün serverin əsas parametrlərinin bəzilərini dəyişdirmək imkanı yaradır.



Şəkil 6.8 "Terminal Services Confiquration" pəncərəsinin "Server Settings" qovluğu

6.4 Lisenziyalaşdırma (Licensing)

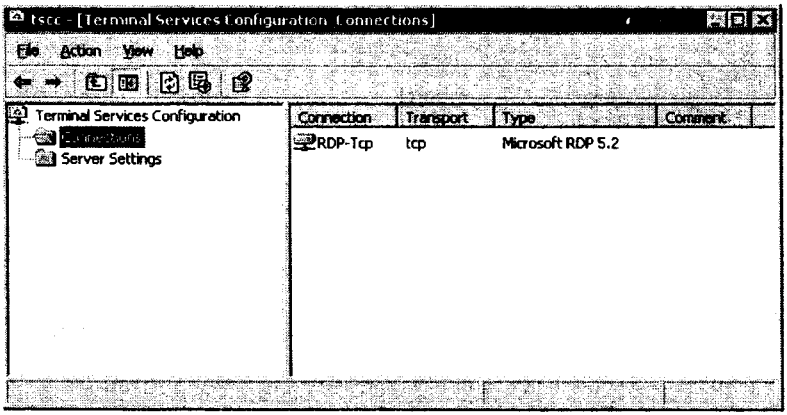
Növbəti sazlama parametri lisenziyalaşdırma rejiminə aiddir. Bu rejim terminal serverin istifadəçilərinin lisenziyalaşdırma serverindən hansı tip lisenziyalar tələb edəcəyinə nəzarət edir.

Praktika göstərir ki, adətən bu rejimə susma prinsipinə görə olan göstəricisi "Per Device" təyin olunur. Bu o deməkdir ki, bunun üçün "Per Device" lisenziyasını, lisenziyalaşdırma serverində quraşdırmaq lazımdır. Əgər korporativ şəbəkəyə məxsus MS Windows Server 2003 əməliyyat sisteminin Terminal Serverini "Internet Connector Licensing" lisenziyasını istifadə edərək yeniləşdirmək tələb olunursa, onda "Per User" lisenziyasından istifadə etmək daha məqsədə uyğundur.

Rejimin seçilməsi birbaşa olaraq iş mühitindən asılıdır. Məsələn, korporativ şəbəkədə elə istifadəçilər vardır ki, onların eyni zamanda bir neçə qurğulara qoşulması məcburidir. Belə olan halda ən optimal variant kimi "Per User" lisenziyalaşdırılmasını seçmək olar. Əgər korporativ şəbəkə daxilində bir kompüterdən bir neçə müxtəlif təyinatlı istifadəçilər istifadə edirsə, onda "Per Device" lisenziyalaşdırılmasını seçmək daha məqsədə uyğundur. "Per Device" lisenziyalaşdırılması o deməkdir ki, bir kompüterdə işləyən bütün istifadəçilər üçün yalnız bir lisenziya markeri tələb olunacaqdır. Əgər "Per User" lisenziyalaşdırılmasını təyin etsək, onda server "Per Device" markerini almış qurğularla daim əlaqə quracaq və bu əlaqəni yoxlamağa davam edəcək.

İstifadəçini bir seansla məhdudlaşdırmaq (Restrict Each User to One Session). Bu funksiyanın işə salınmasından sonra istifadəçilərin serverdə bir neçə seans yaratmasının qarşısı alınır. Bu isə öz növbəsində serverin resurslarına qənaət etməyə imkan verir. Çünki istifadəçi yalnız bir seans qura bilər və bütün proqramlarını yalnız bu seans çərçivəsində işə sala bilər. Əgər korporativ şəbəkənin istifadəçisinə iş masasından kənarda yerləşən hər hansı bir fərdi proqram təminatına birbaşa giriş vermək tələb olunursa, onda istifadəçiyə eyni zamanda bir neçə vasitəni işə salmaq lazım ola bilər. "Citrix MetaFrame" vasitəsi seansın birgə istifadə olunmasını (*session sharing*) dəstəkləyir. Bu istifadəçiyə eyni serverdə bir seans çərçivəsində bir neçə dərc

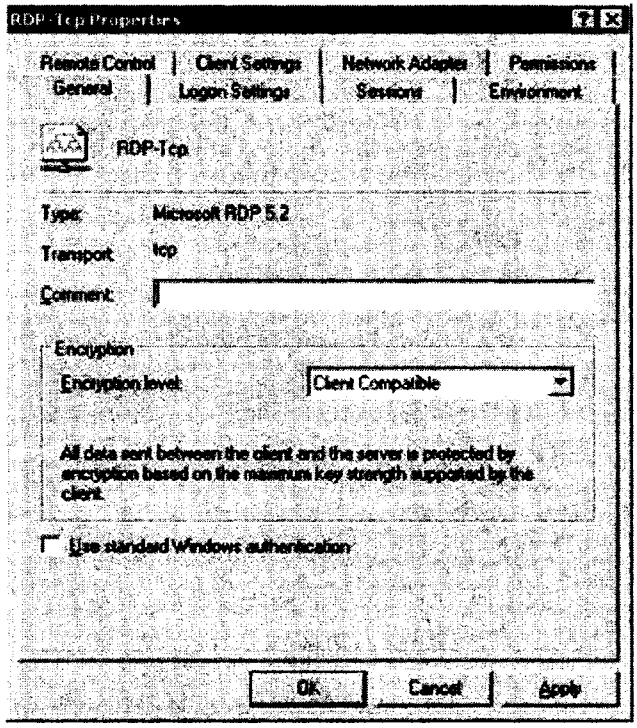
olunmuş proqramları işə salmaq imkanını verir və beləliklə, yeni seansların yaradılmasına heç bir ehtiyac qalmır.
Növbəti şəkildə (şəkil 6.9) bağlantı qovşağı əks etdirilmişdir. Bu qovşaqda sistem administrator "time-out" göstəricisini, təhlükəsizlik və istifadəçilərin resurslarının yönəldilməsini sazlaya bilər.



Şəkil 6.9 "Terminal Services Confiquration" pəncərəsinin "Connections" qovluğu

Susma prinsipinə görə bu pəncərədə yalnız bir ədəd "RDP-Tcp" bağlantısını görmək olar. Əgər korporativ şəbəkənin idarəetmə serveri çoxünvanlı (*multihomed*) serverdirsə, onda administrator əlaqənin təyin edilmə qaydasını elə dəyişdirə bilər ki, bu qayda yalnız bir şəbəkə interfeysinə tətbiq olunsun, daha sonra isə digər şəbəkə interfeysləri üçün yeni əlaqə qursun. Əgər korporativ şəbəkədə "Citrix MetaFrame" vasitəsi quraşdırılıbsa, bu pəncərədə "ICA" bağlantısını görmək olar. Bu bağlantıların birinin üzərində sağ düyməni basaraq onun adının dəyişdirilməsi və ya xassələrinə giriş əldə edilməsinə tamamilə qadağa qoymaq olar. Əgər sistem administratorları daha öncə MS Windows Server 2003 əməliyyat sisteminin "Terminal Services Configuration" vasitəsindən istifadə ediblərsə, onda bu interfeys onlara tanış gələcək. Sadəcə

"RDP 5.2" (Remote Desktop Protokol) və "tam təhlükəsizlik" elementinin yeni versiyası kimi bir neçə əlavələr olunmuşdur. "RDP-Tcp" bağlantısının xassələr pəncərəsinin "General" bəndində (şəkil 6.10) bağlantıya şərhlər əlavə etmək və şifrləmənin səviyyəsini müəyyən etmək mümkündür.



Şəkil 6.10 "RDP-Tcp" xassələr pəncərəsinin "Genral" bəndi

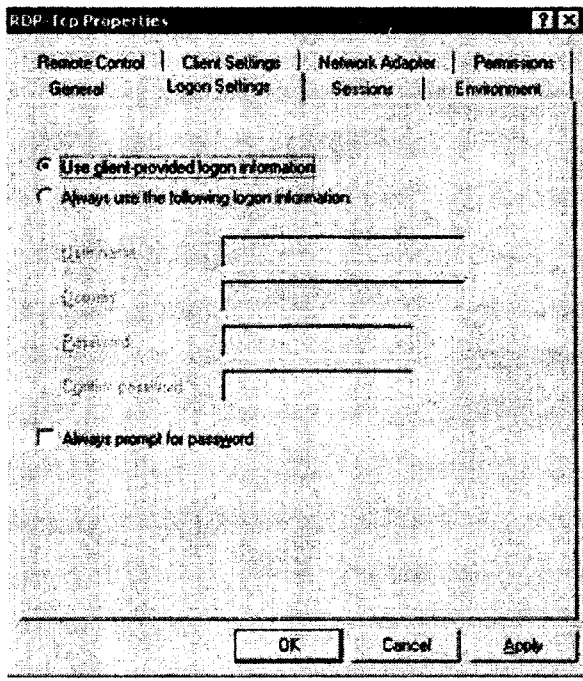
MS Windows Server 2003 əməliyyat sistemi şifrləmənin yeni səviyyələrini təklif edir:

- **Low** – İstifadəçilərdən serverə ötürülən bütün məlumatlar 56 bitlik alqoritm vasitəsi ilə mühafizə olunurlar.
- **Client Compatible** – İstifadəçilərdən serverə ötürülən bütün məlumatlar istifadəçi tərəfindən dəstəklənən açarın maksimal

uzunluğundan istifadə edərək şifrlənirlər.

- **High** – İstifadəçilərdən serverə ötürülən bütün məlumatlar server tərəfindən dəstəklənən açarın maksimal uzunluğundan istifadə edərək şifrlənirlər. İstifadəçilər şifrləmənin bu səviyyəsini dəstəkləyə bilmirlər.
- **FIPS Compliant** – İstifadəçilərdən serverə ötürülən bütün məlumatlar "Federal Information Processing Standard" (FIPS)140-1 standartına uyğun şəkildə şifrlənirlər.

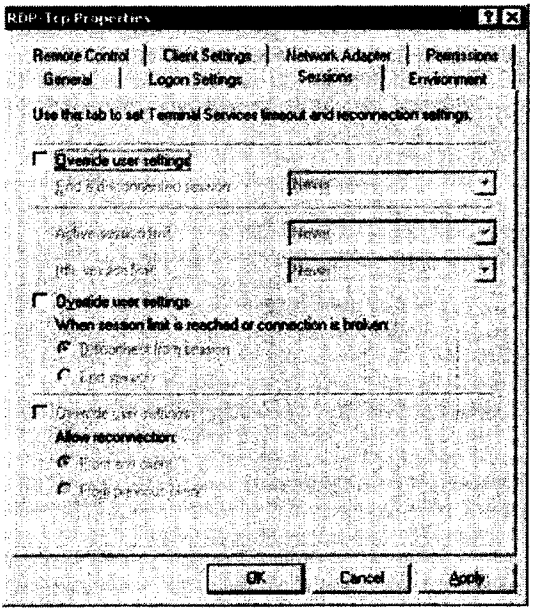
"Logon Settings" bəndində (şəkil 6.11) "İstifadəçinin təqdim etdiyi qeydiyyat məlumatını istifadə et" (Use client provided logon information) funksiyasını və ya "Həmişə aşğıdakı qeydiyyat məlumatını istifadə et" (Always use the following logon information) yazılarının aktivləşdirə bilərlər.



Şəkil 6.11 "RDP-Tcp" xassələr pəncərəsinin "Local Settings" bəndi

Əgər bu pəncərədə "Həmişə aşğıdakı qeydiyyat məlumatını istifadə et" (Always use the following logon information) bəndini aktivləşdirsək, onda sistemə administrator hüququ ilə girmək mümkün olmayacaq.

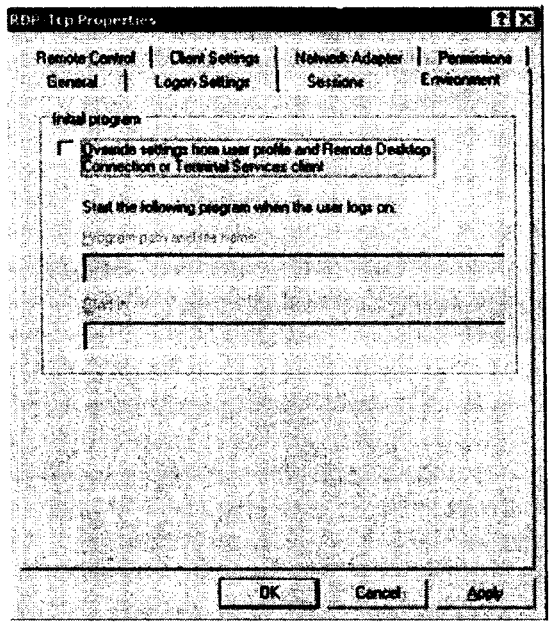
Aşağıda "Sessions" (şəkil 6.12) və "Environment" bəndləri (şəkil 6.13) haqqında məlumat verilir. Bu bəndlərdə adətən "time-out", "yenidən qoşulma" (reconnection) və " İlkin yüklənən proqramlar" (Initial program) funksiyaları aktivləşdirilir. Susma prinsipinə görə bu bəndlər parametrlərin göstəricilərini serverə qoşulan istifadəçinin parametrlərindən götürür. Əgər hər hansı parametrin göstəricisini dəyişmək lazımdırsa, onda bu dəyişikliyi məhz həmin bəndlərdə etmək məqsədə uyğundur.



Şəkil 6.12 "RDP-Tcp" → "Sessions" bəndi

Sessions bəndi kəsilmiş, işlənməmiş və aktiv seanslar zamanı ara kəsilmələri (time-out) özündə cəmləyir. Kəsilmiş seans – bu seans zamanı istifadəçi "Start" menyusundan "Disconnect" bəndini

seçməyərək aktiv şəkildə serverlə əlaqəni kəsir və əlaqə pəncərəsini bağlayır. İşlənməmiş seans – bu seans zamanı əlaqə pəncərəsi açıq olduğuna baxmayaraq verilmiş zaman kəsiyində istifadəçi tərəfindən heç bir əməliyyat yerinə yetirilmir. Əgər cari seans şəbəkə əlaqəsini itirərsə və ya işlənməmiş seansın kəsilməsi hadisəsi baş verərsə, onda iki variantdan birini seçmək olar: 1) seansı tamam bitirmək, 2) cari seansı kəsilmiş seans kimi qəbul etmək.

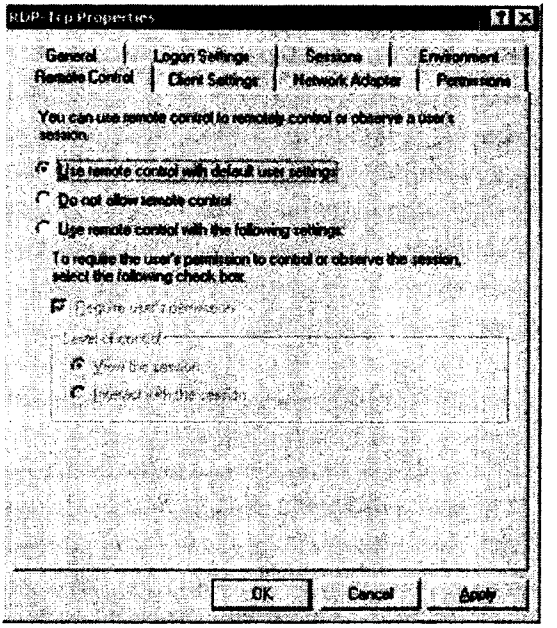


Şəkil 6.13 "RDP-Tcp" → "Environment" bəndi

"Environment" bəndində istifadəçini serverə qoşduqda bəzi proqramların istifadəçi kompüterində işə başlamaq üçün icazə verilib-verilməməsini təyin etmək olar. Burada icra olunacaq faylın həm adını, həm də tam ünvanını göstərmək lazımdır. Bu əməliyyatı yerinə yetirdikdən sonra ixtiyari istifadəçinin, həmçinin administratorun sistemə qoşulduğu zaman Windows Explorer proqramının yerinə "Environment" bəndində göstərilən

proqram açılacaqdır. Lakin bu xidməti heç də "Start" menyusunda olan "Startup" xidməti ilə səhv salmaq olmaz, hansı ki, istifadəçinin sistemə daxil olduğu zaman əvvəlcədən müəyyən olunmuş proqramları avtomatik şəkildə işə salır. Çünki "Environment" bəndində göstərilən proqram, yalnız Windows Explorer proqramının əvəz edir.

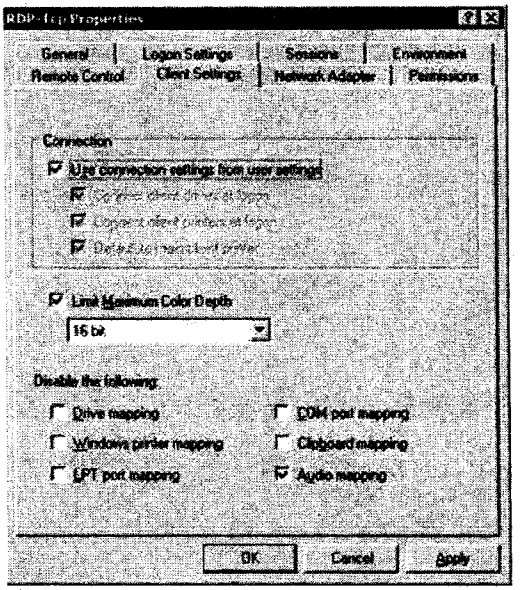
"Remote Control" (şəkil 6.14) və "Client Settings" bəndləri (şəkil 6.15).



Şəkil 6.14 "RDP-Tcp" → "Remote Control" bəndi

Praktikada bəzən, sistem administratorunun mövcud istifadəçi seansına məsafədən qoşulmağı tələb olunur. Bu hal "shadowing" və ya "məsafədən idarəetmə" adlanır. "Remote Control" bəndində parametrlərin göstəricilərini elə sazlamaq olar ki, susma prinsipinə görə öz qiymətlərini istifadəçi parametrlərindən götürsün və ya bu server üçün administrator öz parametrlərini daxil edə bilsin. Bu bəndə parametrləri sazlayan zaman administrator istifadəçinin

seansına məsafədən qoşulmağa icazə verməsi parametrini təyin edə bilər.



Şəkil 6.15 "RDP-Tcp" → "Client Settings" bəndi

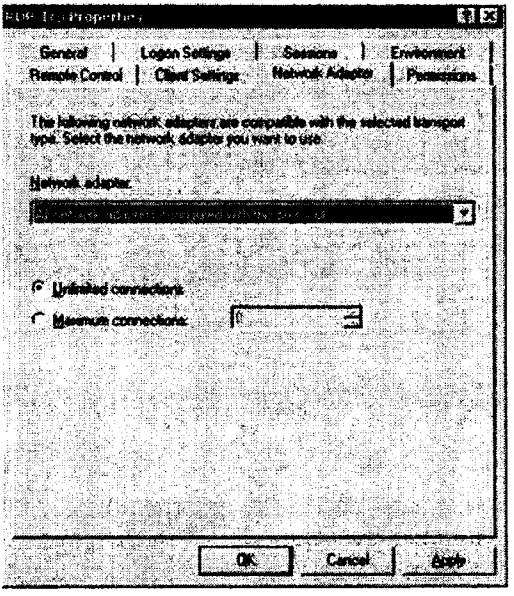
Məsafədən istifadəçi seansına qoşulmanın iki mümkün yolu var: 1) müşahidə və 2) qarşılıqlı əlaqə. "Müşahidə" funksiyası hüququ olan istifadəçilərə digər istifadəçilərin seanslarını idarə və müşahidə etmək imkanı verir. Lakin proqram tərəfindən texniki məhdudiyyətlər qoyulduğundan burada konsol vasitəsi ilə digər istifadəçilərin seanslarını məsafədən idarə etmək mümkün olmur. Əgər "qarşılıqlı əlaqə" funksiyası seçilibsə, onda şəbəkənin administratoru istifadəçinin klaviaturasından və digər idarəetmə qurğularından istifadə edə bilər.

"Client Settings" bəndi isə istifadəçinin aşağıda sadalanan resurslarının yönəldilməsinin yenidən təyin olunmasına imkan verir:

- Drayverlər
- LPT portlar (həmçinin çap qurğuları)

- COM portlar
- Yaddaş buferləri

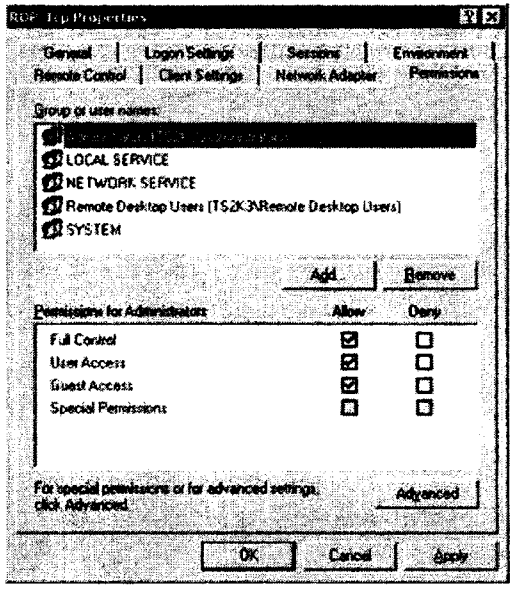
"Network Adapter" (şəkil 6.16) və "Permissions" bəndləri (şəkil 6.17) serverin parametrlərinin sazlanmağına xidmət edirlər. "Network Adapter" bəndi vasitəsi ilə parametrlərin bir və ya bir neçə şəbəkə adapterlərinə şamil olduqlarını təyin etmək olar. "Permissions" bəndində "RDP" (Remote Desktop Protocol) protokolu əsasında hansı istifadəçilərin serverə qoşulmaq icazəsi olduğunu və onların hüquqlarının üstünlük səviyyələrini təyin etmək olar.



Şəkil 6.16 "RDP-Tcp" → "Network Adapter" bəndi

Əgər "Network Adapter" bəndində "All network adapters configured with this protocol" funksiyası aktivləşdirilibsə, bu müəyyən olunmuş şəbəkə adapteri və ya bütün server üçün bağlantıların maksimal sayını məhdudlaşdırmağa imkan verir.

"Permissions" bəndi MS Windows Server 2003 əməliyyat sistemində olan eyni adlı funksiyadan fərqlənir.



Şəkil 6.17 "RDP-Tcp" → "Permissions" bəndi

MS Windows Server 2003 əməliyyat sistemində olan hüquqların təyin olunması funksiyası susma prinsipinə görə bütün etibar olunan domenlərin istifadəçilərinin terminal serverinə qoşulmaq imkanını verir. Lakin MS Windows Server 2003 əməliyyat sistemində təhlükəsizlik anlayışı ixtiyari amildən üstün götürüldüyündən, qoşulma yalnız administratorlara və " Remote Desktop Users" qrupuna aid olan istifadəçilərə şamil olunur. İlkin olaraq "Remote Desktop Users" qrupunun daxili boş olmur və yalnız istifadəçiləri bura əlavə etdikdən sonra onların terminal serverə qoşulmalarını təşkil etmək olar. "Remote Desktop Users" qrupuna daxil olan istifadəçiləri idarə etmək üçün qrup siyasətində yerləşən "Managed Group" vasitəsindən istifadə etmək olar.

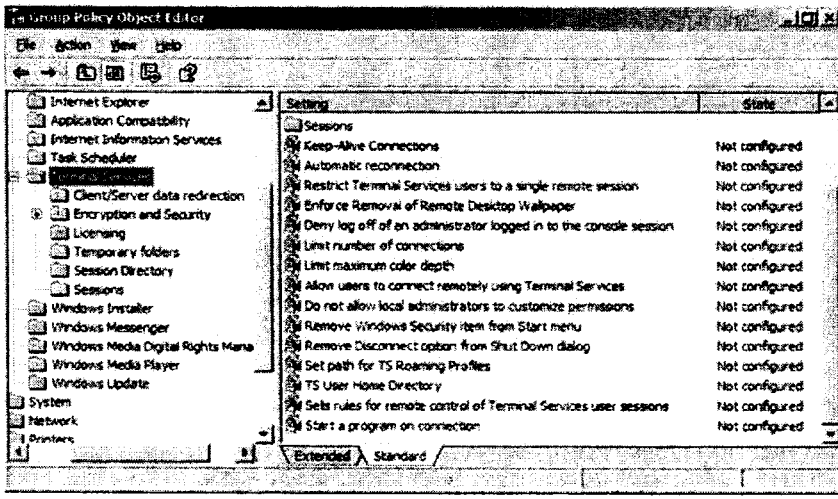
6.5 Qrup siyasətlərinin əsas sazlanması

MS Windows Server 2003 əməliyyat sistemində qrup siyasətlərinin redaktoruna bir sıra yeni parametrlər daxil olunub. Terminal serverin hansı mühitdə yerləşməsindən asılı olmayaraq, terminal serverin quraşdırılma parametrləri lokal kompüter siyasətindən əldə edilə bilər. Bu quraşdırılma parametrləri "Qrup siyasətinin redaktoru" (Group Policy Editor) (şəkil 6.18) vasitəsi ilə redaktə oluna bilər. Qrup siyasətinin lokal redaktoruna giriş əldə etmək üçün komanda sətrindən "gpedit.msc" yazısını daxil etmək kifayətdir. Açılmış pəncərədə "Terminal Services" qovluğunu aşağıdakı qaydada açmaq mümkündür:

Computer Configuration → Administrative Templates → Windows Components →Terminal Services

Sazlama parametrləri bir neçə kateqoriyaya bölünüblər: Encryption (Şifrlənmiş), Licensing (Lisenziyalaşdırılmış), Sessions (Seanslar) və s. Burada bəzi quraşdırılma parametrlərinin "Terminal Services Configuration" pəncərəsində olan parametrlərlə eyni olduğunu görürük. Bu ona görə belə formada realizə olunmuşdur ki, administratorlar serverlərin quraşdırılma parametrlərini mərkəzləşdirilmiş şəkildə idarə edə bilsinlər və hər bir serveri ayrılıqda mexaniki qaydada konfiqurasiya etməyə ehtiyac qalmasın. Quraşdırılma parametrlərindən bəziləri şəkil 6.8-də göstərilmişdir:

Set path for TS Roaming Profiles (yerini dəyişən profillər üçün terminal server marşrutunu təyin olunması). Bu parametr yerini dəyişən profillərin saxlanılması üçün nəzərdə tutulan ümumi istifadə qovluğunu və serveri təyin etməyə imkan verən vasitədir. Həmçinin istifadəçinin hər bir qeydiyyat yazısı üçün terminal serverdə olan ünvanını müəyyən etmək mümkündür. Bu sazlama parametrinin vasitəsi ilə istifadəçi parametrlərini yenidən təyin etməkdən başqa, həm də terminal server və ya terminal serverlər qrupu üçün digər profilləri təyin etmək mümkündür.



Şəkil 6.18 Qrup siyasətinin redaktoru pəncərəsi

Belə yanaşma böyük həcmli korporativ şəbəkələrdə, xüsusən də coğrafi paylanmış ərazidə yerləşən terminal serverlər mühitində və onların daim yer dəyişən istifadəçiləri üçün çox rahat, praktik və iqtisadi baxımdan sərfəlidir.

TS User Home Directory (terminal server istifadəçisinin əsas kataloqu) Bu sazlama parametri əvvəlki parametrə çox oxşayır, əlavə olaraq server və qovluğa terminal serverlərdə qeydiyyatdan keçən istifadəçilər üçün əsas kataloqun yaradılması göstərişini verir.

Yuxarıda göstərilən parametrlərdən birini sazlayaraq hər bir istifadəçi üçün müvafiq kataloq göstərməyə çalışmaq lazım deyil. Server özü avtomatik olaraq marşrutun əvvəlinə **%username%** işarəsini əlavə edəcək.

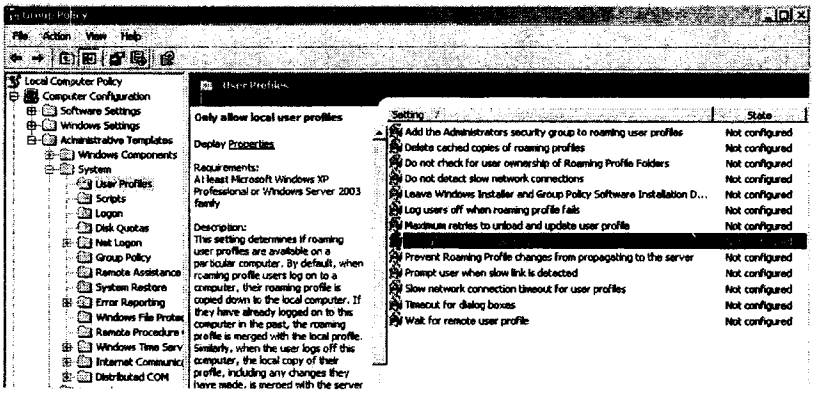
Do not allow local administrators to customize permissions (lokal administratorlara hüquqların dəyişdirilməsinə icazə verməmək). Sözü gedən sazlama parametri aktiv olanda "Terminal Services Configuration" pəncərəsində "Permissions" bəndindən istifadə qadağan olur. Çünki MS Windows Server 2003

əməliyyat sistemində olan "RDP" (Remote Desktop Protokol) protokolunun susma prinsipinə görə imkanları məhduddur. Adətən isə istifadəçilərin terminal serverlə əlaqəsini yaratmaqdan ötrü həmin istifadəçiləri "Remote Desktop Users" qrupuna əlavə edərək əlaqəni yaradırlar. Lakin bu bəndi tamamilə qadağan etmək də mümkündür.

"Terminal Services" bölməsində olan "Licensing" bəndi terminal xidmətlərin lisenziyalaşdırması serverini sazlamaq üçün istifadə olunur. "Licensing" bəndinin köməyi ilə terminal xidmətlərin lisenziyalaşdırılmasına təhlükəsizlik qrupları və ya lisenziyaların yeniləşdirmək qadağasını tətbiq etmək olar. Təhlükəsizlik qrupları lisenziyalaşdırma serverini yalnız o terminal serverlərin markerlərinə verilməsini məcburi edir ki, o serverlər "Terminal Services Computers" təhlükəsizlik qrupunun üzvü olsunlar. Lisenziyaların yeniləşdirilməsinə qoyulan qadağa MS Windows 2000 Server əməliyyat sistemli serverə qoşulan MS Windows Server 2003 əməliyyat sisteminin istifadəçilərinə terminal lisenziyaların markerlərinin verilməsinin qarşısını alır. Susma prinsipinə görə, əgər lisenziyalaşdırma serverinin MS Windows 2000 Server əməliyyat sistemi üçün istifadədə olunan lisenziyası yoxdursa, onda bu server MS Windows Server 2003 əməliyyat sisteminə məxsus lisenziyalardan istifadə edir.

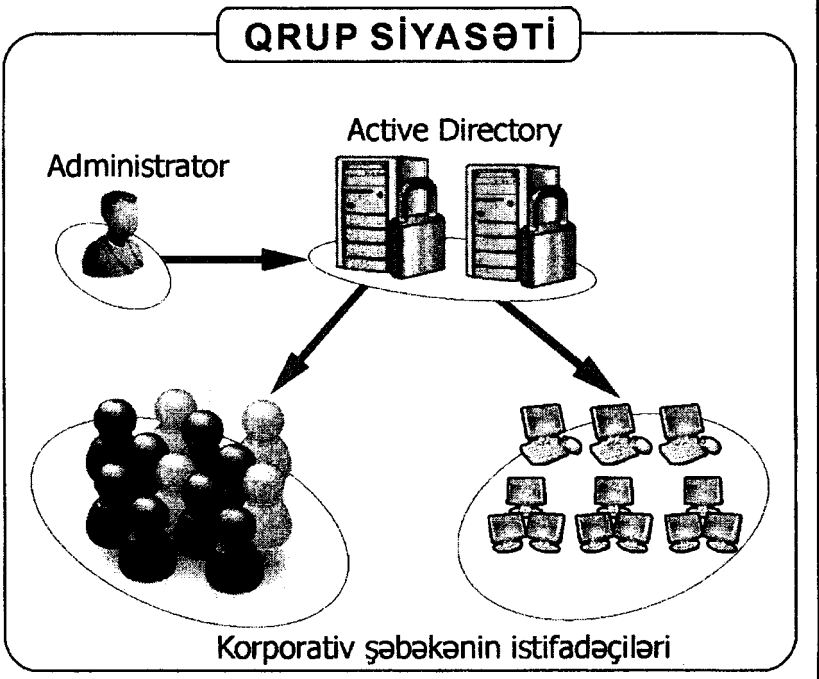
"Session Directory" bəndi seanslar kataloqunun klasterinin üzvü olan terminal serverlərinin konfiqurasiyası üçün istifadə olunur. Bu bənddə şəbəkə administratoru klasterin adını və seanslar kataloqunun serverini və s. parametrləri təyin edə bilər.
Terminal serverin administratorları üçün bir neçə sazlama parametrləri mövcuddur.
Computer Configuration → Administrative Templates → System → User Profiles qovluğunda "Only allow local user profiles" (ancaq lokal istifadəçi profillərinə icazə verilməsi) bəndi (şəkil 6.19) vardır. Bu parametr, serveri yerini dəyişən profillərin

yüklənməsindən azad edir, hətta onlar istifadəçinin qeydiyyat yazılarında təyin olunubsa belə.



Şəkil 6.19 Qrup siyasətinin redaktoru pəncərəsində "User Profiles" qovluğunun "Only allow local user profiles" bəndi

"User Profiles" bəndi həmçinin "Delete cached copies of roaming profiles" siyasətini özündə saxlayır. İstifadəçi sistemdən çıxdığı zaman, bu siyasət serverə yerini dəyişən profilin lokal nüsxəsinin silinməsi əmrini verir. Belə yanaşma serverin daimi yaddaşında həm yerə qənaət etməyə və həm də profilin köhnə versiyası ilə şəbəkə versiyasının birləşməsinin qarşısını almağa imkan verir. Məsafədən idarəetmənin sazlama parametrləri, "time-out" göstəriciləri və mühitin parametrləri "Computer Configuration" bəndində olduğu kimi **User Configuration → Administrative Templates → Windows Components → Terminal Services** bəndində də görmək olar. Belə ikili yanaşma istifadəçi səviyyəsində siyasətləri sazlamaq üçün nəzərdə tutulmuşdur. Əksər hallarda əgər korporativ şəbəkənin administratoru eyni sazlama parametrlərini həm "Computer Configuration" bəndində, həm də "User Configuration" bəndində təyin edibsə, onda əməliyyat sistemi "Computer Configuration" bəndinin parametrlərini əsas götürür.



FƏSİL 7

KORPORATİV ŞƏBƏKƏLƏRDƏ QRUP SİYASƏTİ

KORPORATİV ŞƏBƏKƏLƏRDƏ QRUP SİYASƏTİ

- Qrup siyasətinin idarə olunması
- Domenlərin idarə olunması
- Şəbəkə bağlantılarının sazlanması parametrləri
- Meşələrarası etibar münasibətləri
- Təhlükəsizlik elementlərinin imkanları
- Korporativ şəbəkənin idarəetmə elementləri
- Korporativ şəbəkənin idarəetmə mexanizmində instrumental vasitələr
- Korporativ şəbəkənin funksionallığı

Fəsil 7. KORPORATİV ŞƏBƏKƏLƏRDƏ QRUP SİYASƏTİ

Korporativ şəbəkənin MS Windows Server 2003 əməliyyat sistemi vasitəsi ilə idarə edilməsində müxtəlif yanaşmalar mövcuddur. Bunlardan birini, yəni qrup siyasəti və ona uyğun instrumental vasitələr ilə şəbəkə istifadəçilərinin və bəzi şəbəkə xidmətlərinin idarə olunması bu fəslin əsasını təşkil edir.

7.1 Qrup siyasətinin idarə olunması

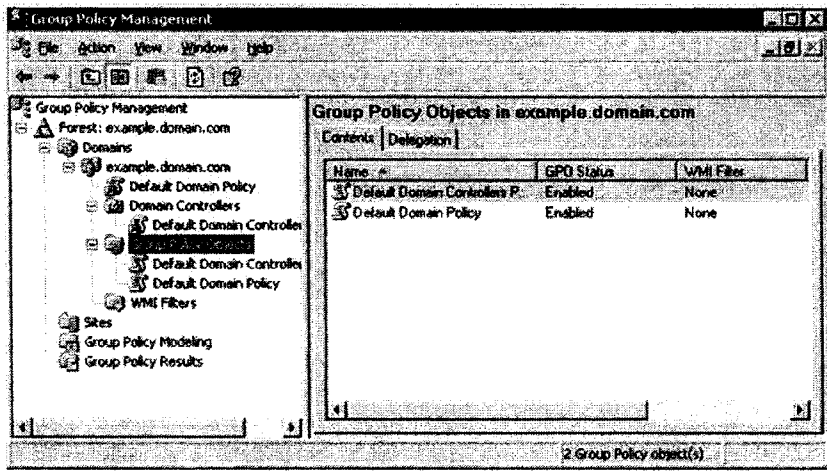
Microsoft Group Policy Management Console (GPMC) – qrup siyasətinin (Group Policy) idarə olunması üçün artıq yeni bir vasitədir (şəkil 7.1). Bu vasitənin köməyi ilə ixtiyari arxitekturaya malik korporativ şəbəkənin idarə olunmasına yönəlmiş xərcləri azaltmaq mümkündür. GPMC vasitəsinin tərkibinə Microsoft Management Console (MMC) və ssenarilər vasitəsi ilə həyata keçirilən qrup siyasətini idarə etmək üçün interfeyslər yığımı daxildir. Burada tərkib element olan "Qrup siyasətinin obyekti" - Group Policy Object (GPO) – Windows əməliyyat sistemləri ailəsində Active Directory xidmətində işçi stansiyaların və məsafədən qoşulan istifadəçilərin konfiqurasiyalarının mərkəzləşdirilmiş şəkildə idarə edilməsindən ibarətdir. GPMC vasitəsi əməliyyat sistemindən ayrı bir komponent kimi reallaşdırılmışdır. GPMC vasitəsi əsasən aşağıda sadalanan məsələlərin həlli üçün nəzərdə tutulub:

• İdarəetmənin bütün əsas elementlərini vahid bir nöqtədə toplamaqla qrup siyasəti vasitəsi ilə idarəetmənin sadələşdirilməsi. Ümumiyyətlə GPMC vasitəsini qrup siyasətinin vahid mərkəzləşdirilmiş idarəetmə nöqtəsi kimi qəbul etmək olar.

• İstifadəçilərin qrup siyasətinə olan əsas tələblərinin reallaşdırılması, aşağıda sadalananlar vasitəsi ilə həyata keçirilməsi mümkündür:

* qrup siyasəti ilə işləməyin asanlaşdırılmasını təmin edən istifadəçi interfeysi;

* ehtiyat nüsxənin çıxarılması və qrup siyasəti obyektlərinin (Group Policy Object – GPO) bərpası;
* qrup siyasətinin obyektləri üçün idxal və ixrac əməliyyatlarının, "Windows Management Instrumentation" (WMI) vasitəsi üçün dəstək süzgəclərinin reallaşdırılması;
* qrup siyasəti ilə bağlı olan təhlükəsizlik aspektlərinin idarə olunmasının sadələşdirilməsi;
* GPO vasitəsinin parametrlərinin HTML (Hypertext Markup Language) formatında hazırlanması;
* "Policy Results" və "Group Policy Modeling" vasitələrinin verilənlərini HTML formatında hazırlanması;
* GPO vasitəsi üzərində əməliyyatların ssenarilərin köməyi ilə həyata keçirilməsi. GPMC vasitəsinə qədər korporativ şəbəkənin administratorları qrup siyasəti vasitəsi ilə idarəetməni bir neçə müxtəlif təyinatlı sistem proqramları istifadə etməklə həyata keçirirdilər. İndi GPMC vasitəsi bütün bu sistem proqramlarını bir araya inteqrasiya edir, vahid bir idarəetmə konsolu və bu sistem proqramlarının təklif etdiyi imkanların genişləndirilməsini təklif edir.



Şəkil 7.1 GPMC pəncərəsi

7.2 Domenlərin idarə olunması

GPMC vasitəsi, Active Directory xidməti quraşdırılmış MS Windows 2000 Server və MS Windows Server 2003 əməliyyat sistemlərində domenləri idarə etməyə imkan verir. Hər iki halda bu vasitənin yerinə yetirilməsi üçün korporativ şəbəkənin administratorunun kompüterində ya "Service Pack 2" (SP2), "post-SP2 hot fix" quraşdırılmış MS Windows Server 2003 əməliyyat sistemi, ya da "Microsoft .NET Framework" vasitələri olan MS Windows XP Professional əməliyyat sistemi quraşdırılmalıdır.

Active Directory vasitəsində qrup siyasətinin dəstəklənməsinin aşağıdakı üstünlükləri vardır:

• MS Windows Server 2003 əməliyyat sistemində yeni istifadəçilər və kompüterlərin konteyneri, yeni obyektləri təyin olunmuş təşkilati bölməyə yönəldilməsi funksiyalarını özlərində cəmləşdirirlər. Məhz burada onlara qrup siyasətinin qaydaları şamil oluna bilər. Belə yanaşma yeni obyektlərin domeninin ilkin səviyyəsində standart konteynerdə qalması hallarının qarşısını tam almış olur. Belə tip konteynerlər qrup siyasətinin əlaqələrini qoruyub saxlamaq üçün nəzərdə tutulmamışdır və istifadəçilər bu konteynerdən qlobal siyasəti nə əldə edə bilirlər, nə də tətbiq edə bilirlər. Nəticə etibarı ilə bu tip konteyneri istifadə edən istifadəçilər üçün domen səviyyəsində qaydaları təyin etmək mümkündür. Belə yanaşma öz çətin tətbiqi ilə adətən korporativ şəbəkənin administratorları üçün problemlər yaratmağa başlayır. Lakin çıxış yolu kimi yenidən yaradılan obyektlərin saxlanılması üçün təşkilati bölmələrin məntiqi iyerarxiyasının yaradılmasını göstərmək olar. Mövcud köhnə üç tip "API" üçün susma prinsipinə görə aşağıdakı parametrləri təyin etmək lazımdır: "NetUserAdd", "NetGroupAdd" və "NetJoinDomain". Korporativ şəbəkə administratorları bu parametrləri " Resource Kit" vasitəsinin yeni alətləri olan "RedirUsr" və "ReDirComp" elementləri ilə həyata keçirə bilərlər. Belə olan halda susma

prinsipinə görə uyğun gələn təşkilati bölmənin istifadə olunması həm də qrup siyasətinin birbaşa olaraq tətbiq olunması deməkdir.

Realizə olunan qrup siyasəti (Group Policy Results). Realizə olunan qrup siyasəti korporativ şəbəkənin administratorlarına obyektə tətbiq olunan cari siyasətin qaydalarını analiz etmək imkanını verir. Burada administratorlar cari siyasətin qaydalarına istifadəçilərin kompüterlərində baxmaq imkanına malikdirlər. Realizə olunan qrup siyasəti bir neçə il bundan öncə "Resultant Set of Policy" vasitəsində qeydiyyatdan keçmə kimi qəbul olunurdu.

Qrup siyasətinin modelləşdirilməsi (Group Policy Modeling). Bu vasitə ssenariləri təyin etmə və onlar üçün siyasətin qaydalarına, proqramlarına və təhlükəsizliyinə baxış keçirməyə imkan verir. Korporativ şəbəkənin administratorları şəbəkə daxilində bir sıra testlər təşkil etməklə müəyyən edə bilərlər ki, istifadəçi və ya istifadəçilər qrupunu digər yerə və yaxud digər təhlükəsizlik qruplarına köçürdükdə onların durumu necə olacaq. Belə bir testin nəticəsində alınan məlumatlar aşağıdakılardan ibarətdir:

- qrup siyasətinin hansı qaydaları tətbiq olunacaq;
- hansı fayllar avtomatik yüklənəcək.

Yuxarıda göstərilən məlumatların əsasında artıq korporativ şəbəkə administratorları əvvəlcədən bir çox addımlarını dəqiq müəyyən edə bilərlər.

Siyasətin yeni parametrləri. MS Windows Server 2003 əməliyyat sisteminin idarəetmə siyasəti 150-dən çox yeni parametrlərə sahibdir. Bu parametrlər əməliyyat sistemini idarə etmək və sazlamaq üçün nəzərdə tutulmuşdur. Yeni parametrlər: əməliyyat sistemində səhvlər haqqında məlumatlarla, Terminal Server ilə, şəbəkə parametrlərinin sazlanması dialoqu ilə, DNS ilə, şəbəkəyə daxil olmaq üçün sorğularla, qrup siyasəti ilə və müxtəlif profillərlə (məsələn, roaming profiles) iş rejiminin yaxşılaşdırılması üçün nəzərdə tutulub.

Administrativ şablonların veb-təsviri. Administrativ şablonların veb-təsviri "Group Policy Administrative Template" vasitəsinin imkanlarını və həmçinin idarəetmə siyasətinin parametrlərinə baxış imkanını daha da genişləndirir. İdarəetmə siyasətinin hər hansı bir parametrini seçdikdə, onun tətbiq olunma imkanları haqqında məlumat birbaşa administrativ şablonların idarə edilməsinin istifadəçi interfeysinin veb-təsvirində ekrana çıxır. Bu verilənləri həmçinin idarəetmə siyasətinin hər bir parametrinin xassələri pəncərəsində yerləşən "Expand" bölməsində əldə etmək mümkündür.

DNS istifadəçisinin idarə olunması. MS Windows Server 2003 əməliyyat sistemində DNS istifadəçisinin parametrlərini sazlamaq üçün korporativ şəbəkənin administratorları qrup siyasəti elementlərindən istifadə edə bilərlər. Bu isə öz növbəsində domen üzvlərinin parametrlərinin konfiqurasiya olunmasını asanlaşdırır. Bu parametrlərə misal olaraq istifadəçilərin DNS yazılarının dinamik qeydiyyat işini başlamaq və dayandırmaq, ilkin DNS serverinində adların icazə verilməsi zamanı suffiksin əvəz olunmasının (devolution) tətbiqini və DNS suffikslərinin axtarış siyahılarının doldurulmasını göstərmək olar. DNS suffiks dedikdə şəbəkəyə qoşulan işçi stansiyanın şəbəkə adapterinin modeli, fiziki ünvanı, DHCP-nin durumu, IP ünvanı, altşəbəkənin maskası və əsas şlyuzu nəzərdə tutulur.

My Documents qovluğunun yönəldilməsi. İstifadəçiləri köhnə tip ana kataloqu modelindən yeni sayılan "Mənim sənədlərim" (My Documents) adlanan qovluğa yönəltmək imkanını verir. Bu yeni model köhnə mühitlə tam uyuşan bir texnologiya əsasında işləyir.

Korporativ şəbəkəyə daxil olan zaman istifadəçi üçün təyin olunan proqram təminatlarının tam quraşdırılması. "Application Deployment Editor" vasitəsi istifadəçi korporativ şəbəkəyə daxil olan zaman, onun üçün əvvəlcədən administrator tərəfindən təyin olunan proqram təminatlarının tam quraşdırılması

imkanını təqdim edir. Belə olan halda, korporativ şəbəkənin administratoru tələb olunan proqramların avtomatik şəkildə istifadəçi kompüterlərinə quraşdırılacağına tam təminat verə bilər.

Netlogon. "Netlogon" vasitəsi qrup siyasətinin öz daxili parametrlərini MS Windows Server 2003 əməliyyat sistemi olan kompüterlərdə sazlamaq üçün istifadə olunur. "Netlogon" vasitəsinin parametrlərini bu yolla sazlayan zaman domen üzvlərini konfiqurasiya etmək, domen kontrollerinin özünə məxsus yazıların axtarışının dinamik qeydiyyatının dayandırılması və işə salınması, belə yazıların yenilənməsinin dövrlüyünü və bir sıra digər əməliyyatları xeyli asanlaşdırır.

7.3 Şəbəkə bağlantılarının sazlanması parametrləri

MS Windows Server 2003 əməliyyat sistemində şəbəkənin sazlanması parametrlərini özündə cəmləyən interfeysə istifadəçilərin giriş hüququnun məhdudlaşdırılması qrup siyasətinin köməyi vasitəsi ilə mümkündür.

Məlumatların paylanmış emalı siyasəti. WMI (Windows Management Instrumentation) hadisələrinin emalı infrastrukturu paylanmış strukturla işləmək üçün modernləşdirilmişdir. Bu genişlənmənin tərkibinə yazılmanın konfiqurasiya olunmasının komponentləri, süzgəc, korrelyasiya və WMI hadisələrinin daşınmaları daxildir. Müxtəlif proqram təminatının istehsalçıları bu interfeysi və siyasətin qaydalarını təyin etməklə, öz sistemlərinə quraşdıraraq bu sistemin faydalı iş qabiliyyətinin monitorinqini, hadisələrin qeydiyyatını, bildirişləri, avto-bərpaları və müxtəlif hesabatları əldə edə bilərlər.

Credential Manager vasitəsi. Bu yeni alət istifadəçilərin qeydiyyat yazılarının idarə olunmasını asanlaşdırmaq üçün nəzərdə tutulub. Qrup siyasətinin qaydaları çərçivəsində "Credential Manager" vasitəsini işə salmaq və dayandırmaq kimi funksiyalar mövcuddur.

Proqram vasitələrinin açılması zamanı URL dəstəklənməsi. İxti yari paket proqramlar üçün URL dəstək vasitələri təklif edir. "Add or Remove Programms" menyusundan hər hansı bir proqramı quraşdırdıqda "Support Information URL" funksiyasını aktivləşdirmək olar. Belə yanaşma, korporativ şəbəkə daxilində istifadəçilər tərəfindən texniki dəstək şöbəsinə müraciətlərin sayının kəskin azaldılmasına gətirib çıxaracaq.

WMI süzgəcləri. WMI vasitəsi verilmiş kompüter üçün böyük həcmli məlumatları, məsələn, korporativ şəbəkənin aparat və proqramların siyahısı, parametrləri və konfiqurasiya məlumatları kimi verilənləri generasiya edir. WMI vasitəsi verilənlərin mənbəyi kimi reyestri, drayverləri, fayl sistemini, Active Directory, Simple Network Management Protocol (SNMP), Windows Installer xidmətini, SQL dilini, altşəbəkə sistemini və Exchange Server vasitəsini istifadə edir. MS Windows Server 2003 əməliyyat sistemində "WMI Filtering" vasitəsi GPO xidmətini WMI verilənlərinə olan sorğularına tətbiq edib-etməyəcəyini dinamik təyin etməyə imkan verir. Bu sorğular həmçinin GPO vasitəsi daxilində hansı kompüterlərin və istifadəçilərin idarəetmə siyasətinin parametrlərini almaq hüququna malik olduğunu təyin edir. Bu funksiyanın köməyi ilə lokal kompüter əsasında qrup siyasətinin konkret məqsədini təyin etmək imkanı mövcuddur. Məsələn, belə bir GPO vasitəsi mövcud ola bilər ki, MS Office XP proqram paketini istifadəçilərə təyin etsin. Lakin korporativ şəbəkənin administratoru şəbəkəyə məxsus olan bütün kompüterlərin disklərində MS Office XP paketi üçün bəs qədər yer olduğuna əmin deyil. Belə olan halda GPO vasitəsi üçün WMI süzgəcini işə salmaq lazımdır. Bu süzgəc MS Office XP paketini yalnız o istifadəçilərə yükləməyə başlayır ki, onların kompüterlərinin əsas yaddaşında 400 Mb-dan çox yer olsun.

Təhlükəsizlik elementləri. MS Windows Server 2003 əməliyyat sistemində Active Directory sistem vasitəsinin dəstəklənməsi təhlükəsizlik elementləri ilə daha da

zənginləşdirilmişdir. Bu təhlükəsizlik elementləri öz növbələrində şəbəkələrarası domenlərin və şəbəkələrdə domenlərarası etibar münasibətlərinin idarə olunmasını asanlaşdırır. Digər tərəfdən, yeni vasitə olan "Credential Manager" istifadəçilərin və "X.509" sertifikatlarının qeydiyyat yazılarının təhlükəsiz saxlanılması servisini təklif edir.

7.4 Meşələrarası etibar münasibətləri

Meşələrarası etibar münasibətləri (forest trust) meşələrin təhlükəsizlik problemlərinin idarə olunmasını asanlaşdırır. Etibar edən meşə istifadəçilərin adlarına məhdudiyyətlər qoymaq hüququna malikdir və bu istifadəçilərin autentifikasiyasını digər meşələrə etibar edir. Onların əsas xassələri aşağıda sadalanır:

- bir meşənin domenlərinin hamısı digər meşənin bütün domenlərinə o zaman etibar edə bilərlər ki, bu iki meşənin əsas iki domeni arasında vahid qarşılıqlı etibar münasibətləri təyin edilmiş olsun;
- burada üç və ya daha çox meşələr arasında tranzitivlik prinsipi işləmir, yəni əgər X meşəsi Y meşəsinə etibar edirsə və Y meşəsi Z meşəsinə etibar edirsə, bu heçdə o demək deyil ki, X meşəsi Z meşəsinə etibar edir və ya əksinə;
- bu münasibətlər bir və ya ikitərəfli ola bilərlər;
- yeni quraşdırılma vasitəsi ilə yaradılan ixtiyari tip etibar münasibətlərinin yaradılması prosesini asanlaşdırır;
- yeni xassələr pəncərəsi meşələrarası etibar münasibətləri ilə bağlı olan adların etibarlı fəzasını (trusted namespace) idarə etməyə imkan verir;
- adların etibarlı fəzaları, autentifikasiya sorğularının yönəldilməsi və meşəni idarə edən qeydiyyat yazılarının mühafizə iştirakçılarının avtorizasiyası məqsədlərinə qulluq edirlər;
- meşə tərəfindən müəyyən olunan domen adları fəzası, istifadəçi identifikatorları (User Principal Name - UPN), xidmət (servis) identifikatorları (Service Principal Name - SPN) və təhlükəsizlik

identifikatorları (Security Identifier - SID) meşələr arasında etibar münasibətlərini təyin edən zaman avtomatik olaraq toplanırlar və Active Directory vasitəsinin istifadəçi interfeysi "Active Directory Domains And Trust" vasitəsi ilə yeniləşdirilirlər;

• meşə tərəfindən müəyyən olunan etibar münasibətləri fəzası "ilk gələn, ilk xidmət olunar" (First Input First Output - FIFO) prinsipinə əsaslanır. Sistemdə mövcud meşələrarası etibar münasibətlərindən olan adların etibarlı fəzasının ilk konflikti baş verən zaman, cari əməliyyat dayandırılır;

• adların etibarlı fəzalarının işinin dayandırılmasının qarşısını avtomatik şəkildə almaq olar. Burada korporativ şəbəkənin administratorları ayrı-ayrı adların etibarlı fəzalarının işini dayandıra bilmək hüququna malikdirlər.

7.5 Təhlükəsizlik elementlərinin imkanları

Active Directory vasitəsində təhlükəsizlik amilinə böyük yer ayrılmışdır, bu amillin elementləri aşağıdakılardır:

• **Meşələrarası autentifikasiya.** Bu vasitə, istifadəçinin qeydiyyat yazıları bir meşədə, kompüterin qeydiyyat yazıları isə digər meşədə yerləşən zaman resurslara təhlükəsiz girişi təmin edir. Belə yanaşma zamanı istifadəçilər digər meşədə yerləşən resurslara "Kerberos" və ya "NTLM" tətbiq edərək təhlükəsiz giriş əldə edə bilərlər və bu zaman istifadəçinin məxsus olduğu meşənin vahid qeydiyyat yazısının və parolunun idarə edilməsinin sadəliyi tam şəkildə qorunub saxlanılır. Meşələrarası autentifikasiyanın aşağıdakı imkanları mövcuddur:

* **Adlara icazə verilməsi** - əgər "Kerberos" və ya "NTLM" lokal kompüter vasitəsi ilə təhlükəsizlik iştirakçısının adına icazə verə bilmirsə, o zaman qlobal kataloqa müraciət olunur. Əgər qlobal kataloq da bu təhlükəsizlik iştirakçısının adına icazə verə bilmirsə, onda yeni funksiya olan "adların meşələrarası qarşılaşdırılması" funksiyası çağırılır və adların qarşılaşdırılması

funksiyası təhlükəsizlik iştirakçılarının adlarını etibarlı fəzalara məxsus bütün meşələrdə olan adları ilə müqayisə edir. Əgər axtarış zamanı meşələrin adları üst-üstə düşərsə, onda həmən ad ünvan kimi yenidən istifadəyə göndəriləcəkdir (routing hint).

* **Sorğuların yönəldilməsi** – "Kerberos" və "NTLM" autentifikasiya sorğularının etibar münasibətləri əsasında ilkin domendən nəzərdə tutulan domenə ötürülməsi üçün yönəltmə ünvanlarından istifadə edirlər. Kerberos üçün açarların paylanma mərkəzi (Key Distribution Center, KDC) etibar münasibətlərinin yerləşdiyi ünvana istinadları (link) generasiya edir və istifadəçilər Kerberos standart alqoritmləri istifadə etməklə bu istinadlara əsaslanırlar. "NTML" üçün domen kontrolleri etibar münasibətlərindən istifadə edərək mühafizəli kanal vasitəsi ilə sorğular göndərməyə başlayır. Sorğuların göndərilməsi şəffaf autentifikasiya (pass-through) tətbiq etməklə həyata keçirilir.

* **Dəstəklənən autentifikasiya** - digər meşənin məsafədə yerləşən serverində autentifikasiyanı dəstəkləyən metodlar arasında "Kerberos" və "NTLM" şəbəkə qeydiyyatları, NTLM interaktiv qeydiyyatları, istifadəçinin məxsus olmadığı meşədə fiziki qeydiyyatı, digər meşələrdə çoxsəviyyəli proqram təminatlarının Kerberos nümayəndələrinə ayrılması metodu vardır. Burada "UPN" (Unified Public Network) qeydiyyatının bütün parametrləri dəstəklənir.

• **Meşələrarası avtorizasiya.** Korporativ şəbəkənin administratorlarına, istifadəçi və ya qrupları lokal qruplara daxil etmək üçün etibarlı meşələrdən asanlıqla istifadə etməyə imkan yaradır. Meşələrarası avtorizasiya, meşənin təhlükəsizlik sərhədinin tamlığını dəstəkləyərək, həmçinin meşələr arasında etibar münasibətləri quramağa imkan yaradır. Bu vasitə etibarlı meşələrdən olan istifadəçilərin mühafizə olunan resurslarına müraciət etdikdə, etibar edən meşəyə icazə verilən təhlükəsizlik

identifikatorlarının siyahısını (Security Identifier - SID) məhdudlaşdırmağa imkan yaradır.

• **Qruplarda üzvlük və ACL (Access Control List) idarəetmə.** Obyektlərin seçilməsi siyahısına etibar olunan meşə istifadəçilərinin və qruplarının adlarının seçilməsi dəstəyi daxil olunmuşdur. Adlar tam şəkildə klaviaturadan daxil olunmalıdır. Şablon üzərində sadalanma və axtarış isə bu vasitə tərəfindən dəstəklənmir.

• **Translyasiya** «ad-SID». ACL obyektlərin seçilməsi və redaktə olunması sistem API vasitələrini istifadə edir və SID identifikatorlarını qrupun üzvlük yazılarına daxil edir. API translyasiyaları «ad-SID» meşələrarası ünvanların yönəldilməsi məqsədi ilə istifadə olunması üçün genişləndirilmişdir. Həmçinin NTLM mühafizəli kanalları domen kontrollerlərinin arasında təhlükəsizlik iştirakçılarının adlarına icazə verilməsi üçün etibar münasibətlərini tətbiq edir.

• **SID süzgəc.** Etibar olunan meşənin əsas domenindən etibar edən meşənin əsas domeninə yoxlanılmış verilənlərin ötürülməsi zamanı SID süzgəc işə düşür. Etibar edən meşə yalnız etibar etdiyi meşənin domenlərindən SID identifikatorunu öz domeni üçün qəbul edir. Yerdə qalan digər SID identifikatorlar avtomatik olaraq inkar olunurlar. SID süzgəc avtomatik olaraq Kerberos və NTLM autentifikasiyası üçün realizə olunur.

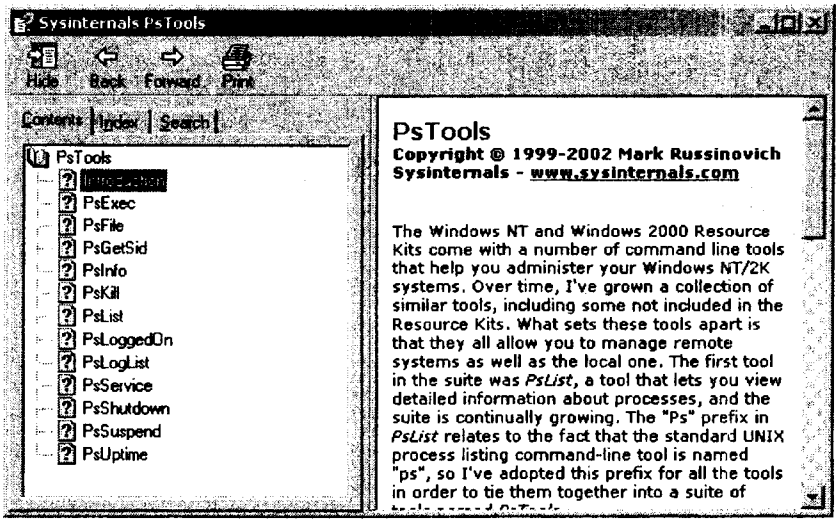
• **Kross-sertifikatlaşma.** Qlobal səviyyədə kross-sertifikatlaşmanı tətbiq edərək, bu vasitənin imkanlarını daha da genişləndirmək mümkündür. Məsələn, artıq "Win-Logon" vasitəsi kross-sertifikatlaşmanı məhdudlaşdıra bilər və onları "enterprise trust/enterprise store" kimi yükləyə bilər. Qurulmuş məntiqi ardıcıllığa əsasən bütün nəzərdə tutulan kross-sertifikatlar yüklənməyə başlayacaqlar.

• **IAS və meşələrarası autentifikasiya.** Active Directory vasitəsinə məxsus meşələr, meşələrarası ikitərəfli etibar münasibətləri rejimində işləyən zaman "Internet Authentication Service/Remote Authentication Dial-In User Service" (IAS/RADIUS) xidməti, istifadəçini digər meşədə autentifikasiya edə bilər. Belə yanaşma korporativ şəbəkələrin administratorlarına yeni meşələri mövcud IAS/RADIUS servisləri ilə asanlıqla inteqrasiya etməyə imkan yaradır.

• **Qeydiyyat yazılarının idarə olunması.** "Credential Manager" vasitəsi istifadəçilərin qeydiyyat yazılarının, parollarının və X.509 sertifikatlarının mühafizəli saxlanma bazasını təqdim edir. Belə yanaşma zamanı korporativ şəbəkədə bütün istifadəçilər üçün vahid qeydiyyat sistemin aparılması mümkün olur. Məsələn, istifadəçinin öz şəbəkəsindən fərqli bir şəbəkədə yerləşən, lazım olan proqram təminatına ilk dəfə müraciət etdiyi zaman hökmən autentifikasiya tələb olunacaq və istifadəçiyə öz qeydiyyat parametrlərini daxil etmək təklif olunacaq. Bu autentifikasiya məlumatlarını daxil etdikdən sonra istifadəçi lazım olan proqram təminatından istifadə edə bilər. Bu proqram vasitəsinə növbəti müraciətlər zamanı istifadəçinin ilk dəfə daxil etdiyi qeydiyyat məlumatları avtomatik olaraq sistem tərəfindən nəzərə alınır və yenidən bu məlumatları daxil etməyə heç bir ehtiyac qalmır.

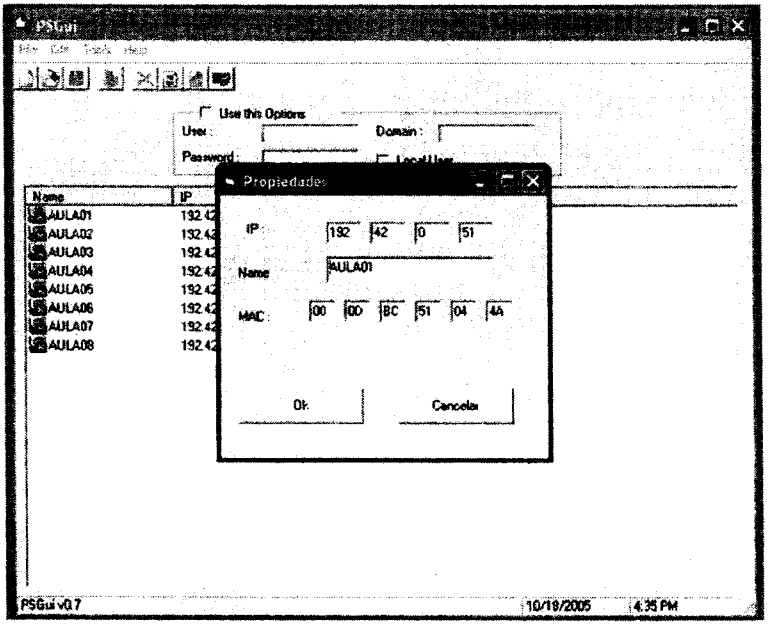
7.6 Korporativ şəbəkənin idarəetmə elementləri

Komanda sətrini tətbiq etməklə məsafədən idarəetmənin praktik baxımdan çox yararlı imkanlarını aşkar etmək mümkündür. Praktika göstərir ki, adətən kənar istehsalçıların şəbəkə proqram vasitələri əməliyyat sisteminin, xüsusən də MS Windows ailəsinə məxsus əməliyyat sisteminin daxilində olan vasitələrə tətbiq olunduqda daha çox əməliyyatlar yerinə yetirmək imkanını əldə etmək olar. Kənar istehsalçıların istehsal etdiyi belə vasitələrdən biri olan "PsTools" paketini göstərmək olar (şəkil 7.2).



Şəkil 7.2 "PsTools Suite 2.43" paketindən fraqment

Bu tip proqramlar MS Windows əməliyyat sistemi ailəsinin server versiyaları üçün nəzərdə tutulmuşdur. Lakin əməliyyat sisteminin daxilində də bir sıra komanda sətri əmrləri mövcuddur. Bu əmrlər vasitəsi ilə bəzi idarəetmə elementlərini həyata keçirmək olur. Son illər qrafik interfeysin yaranması ilə bağlı olaraq artıq bir çox administratorlar komanda sətrindən uzaqlaşmağa başlayıblar. Bu da qrafik interfeysin həddindən artıq anlaşılan, düymələrin məntiqi ardıcıllıqla yerləşdirilməsi və yerinə yetiriləcək addımın aydın şəkildə başa düşülməsi ilə bağlıdır (şəkil 7.3). Əgər qrafik interfeysdə nə isə aydın deyilsə, bunun üçün MS Windows əməliyyat sistemində məlumatlar bölməsi var və bu bölmənin köməyi ilə proqramın və ayrı-ayrı elementlərin işləməsi haqqında dolğun məlumat almaq mümkündür. Lakin komanda sətri qrafik interfeysin tam əksi olaraq istifadəçiləri mərəkkəbliyi ilə özündən uzaq salır. Buna baxmayaraq komanda sətri vasitələri, qrafik interfeysə malik olan proqramlardan bəzi texniki məqamlarda qat-qat üstündür.



Şəkil 7.3 "PsGui" paketinin qrafik interfeysindən fraqment

Hətta korporativ şəbəkənin ən sadə konfiqurasiyaya malik işçi stansiyasında elə hal ola bilər ki, burada komanda sətrindən başqa heç bir vasitə kömək edə bilməz. Deyilənlərə misal olaraq və praktikada tez-tez rast gəlinən, MS Windows əməliyyat sisteminin hər hansı bir işçi stansiyada "Yalnız komanda sətri" rejimində açılması halını göstərmək olar. Çıxış yolu kimi komanda sətri rejimində bu əməliyyat sistemini yükləmək və ya bərpa konsolunu açmaq olar. Göstərilən halları işçi stansiyasının işləmədiyi zaman atılacaq son addımlar kimi qiymətləndirmək lazımdır.

Praktikada belə hallara da rast gəlinir ki, sistem tam şəkildə çalışır, lakin əməliyyat sisteminin qrafik imkanları vasitəsi ilə yerinə yetiriləcək əməliyyatı həyata keçirmək mümkün olmur. Əgər hər hansı bir səhv əməliyyatın nəticəsində külli miqdarda faylların nüsxələri sistemdə mövcuddursa və onları sistemdən qısa bir zamanda silmək tələb olunursa, onda qrafik interfeys metodu

köməyə gələ bilməz. Çünki silinəsi faylların hamısını bir dəfəyə seçib pozmaq mümkün deyil. Əməliyyat sisteminin qrafik rejim üçün təyin etdiyi məhdudiyyətlər mövcuddur. Bu isə o deməkdir ki, bir dəfəyə yalnız bəlli miqdarda fayl seçmək imkanı vardır və külli miqdarda faylların silinməsinə həddindən çox zaman tələb oluna bilər. Bu vəziyyətdən çıxış yolu kimi komanda sətrində olan "del" ə mrini göstərmək olar. Bu əmrin müvafiq parametrlərini təyin edərək, sistemdə lazımsız olan külli miqdarda faylları bir neçə saniyəyə silmək mümkündür. Bu əmrin komanda sətrində yazılışı belədir:

del /s /q c:\ *(faylın axırında olan suffiks).*

Məsafədən idarəetmənin imkanları həddindən artıq genişdir. Lokal işçi stansiyasında tətbiq oluna biləcək bütün əmrlər demək olar ki, hamısı məsafədən idarə olunan kompüterə tətbiq oluna bilərlər. "PsTools" proqramının və əməliyyat sisteminin distributiv diskində yerləşən "Support Tools" paketinin (Resource KIT) bəzi imkanlarını nəzərdən keçirək.

Remote.exe (Support Tools)

"Support Tools" paketinin server əməliyyat sistemi üçün nəzərdə tutulmuş versiyasında "remote.exe" sistem vasitəsi vardır. Bu sistem vasitənin köməyi ilə idarəetmə məsələlərini, komanda sətrindən həyata keçirmək mümkündür. "Remote.exe" sistem vasitəsi ilk öncə korporativ şəbəkənin idarəetmə serverində, sonra isə idarə edilməsi nəzərdə tutulan işçi stansiyada işə salınmalıdır. "Remote.exe" sistem vasitəsi serverdə olan ixtiyari qovluğa köçürdükdən sonra komanda sətrindən həmin qovluğa daxil olub

remote /s "cmd" /v

əmrini daxil edirik.

Burada "s" – "remote.exe" vasitəsinin server hissəsinin işə salınması əmridir, "cmd" – komanda sətridir, "v" – proqramı görünən rejimdə işə salır.

Qoşulmaq tələb olunan işçi stansiyanın komanda sətrində

remote /c <serverin_adı> /v

əmrini daxil etmək lazımdır.

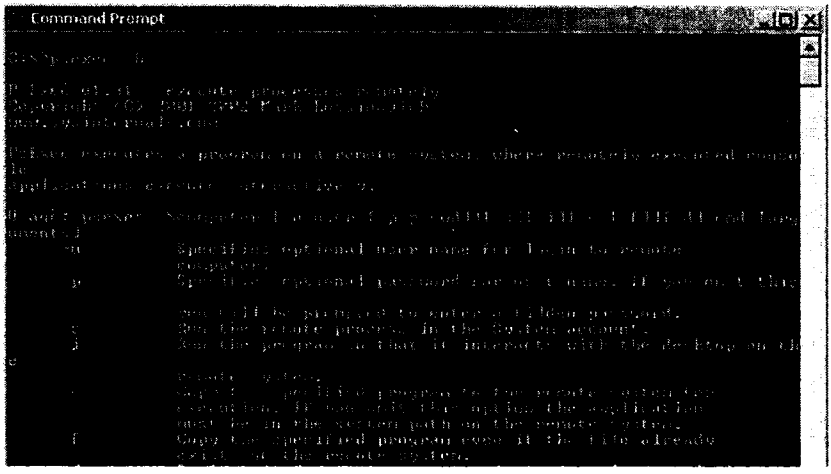
Burada "/c" – parametri istifadəçi kompüterində proqramın işə salınması haqqında məlumat verir.

Beləliklə, proqramın işə salındığı və serverdə yerləşən qovluğuna giriş əldə etmək mümkündür. İndi isə artıq komanda sətrindən ixtiyari əmrləri yerinə yetirmək olar. Burada qovluqlar yaratmaq və ya silmək, faylları bir yerdən digər yerə köçürmək, serverdə IP protokolunun konfiqurasiyasına baxmaq üçün "ipconfig" əmrini və bir sıra digər əmrləri yerinə yetirmək olar.

Bu proqram vasitəsi yalnız latın hərflərini dəstəkləyir və digər əlifbalarla işarələnmiş qovluqlar və faylların adını həmin dildə əks etdirir. Lakin bəzi əmrlərin yerinə yetirilməsini istifadəçi ekranda görməyəcək. Məsələn, mətn faylının tərkibini ekrana çıxarmaq cəhdi onunla nəticələnəcək ki, bu faylın tərkibi serverdə ekrana çıxacaq, amma istifadəçi isə yalnız bu əməliyyatın uğurla yerinə yetiriləcəyi haqqında bildirişi öz ekranında görmüş olacaq. Beləliklə, "type file.txt" əmri tam qaydada realizə olunacaq və lazımı məlumat istifadəçinin ekranında təsvir ediləcək. İstifadəçi kompüterindən yerinə yetirilən bütün əmrlər, bu əməliyyatın nə zaman və kim tərəfindən həyata keçirildiyi haqqında məlumatlar serverdə toplanırlar. Qrafik interfeyslə olan proqram təminatının işə salınması əmrlərin daxil edilməsinin qarşısını alır və serverdə komanda sətri pəncərəsinin bağlanmasına gətirib çıxarır. Serverlə olan əlaqə seansını normal rejimdə bağlamaq üçün "ok" əmrini daxil etmək kifayətdir. Yuxarıda göstərilən bütün amilləri nəzərə alaraq, qeyd etmək lazımdır ki, "remote.exe" sistem vasitəsi korporativ şəbəkənin idarə olunmasında administratora tam köməkçi ola bilər.

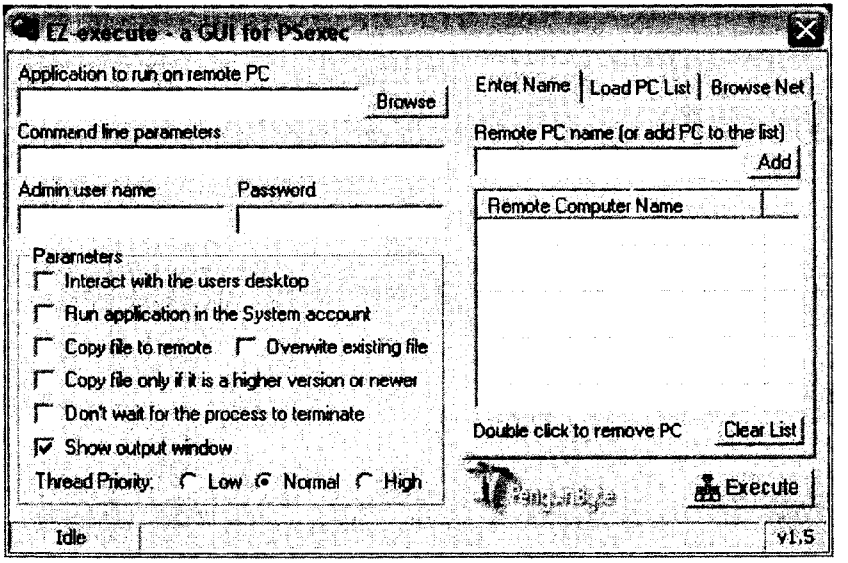
7.7 Korporativ şəbəkənin idarəetmə mexanizmində instrumental vasitələr

- **PsExec (PsTools)** sistem vasitəsinə əlavə olunan texniki parametrlərdə göstərilmişdir ki, bu vasitə məsafədə olan işçi stansiyalarda komanda sətri əməliyyatlarını yerinə yetirməyə imkan verir (şəkil 7.4 – 7.5). Lakin real praktikada bu proqram o qədərdə işə yaramır və məhz onun qeyri-funksional olmasından bu vasitə çox istifadə olunan sistem vasitələri siyahısında deyildir. Bu sistem vasitəsinin tətbiqi zamanı məsafədə olan kompüterə serverlə əlaqə qurmaq üçün lazım olan xidmət quraşdırılmalıdır.



Şəkil 7.4 "PsExec" sistem vasitəsindən fraqment

Lakin MS Windows əməliyyat sisteminin təhlükəsizlik elementlərini yeniləşdirən zaman, bəzən serverlə ə laqə qurmaq üçün lazım olan xidmətlərin yerinə yetirilməsinə qadağalar qoyulur. Nəticə olaraq bu tip xidmətlər qeyri-funksional olaraq sistemdə qalır və şəbəkənin serveri ilə heç bir əlaqə yarada bilmir. Belə olan halda çıxış yolu kimi və "PsExec" vasitəsinin izlərini silmək üçün digər sistem vasitə olan "srvinstw.exe" proqramını göstərmək olar. Bu sistem vasitə əməliyyat sistemində lazım olmayan xidmətləri silməyə imkan verir.



Şəkil 7.5 "PsExec" vasitəsinin qrafik interfeysindən fraqment

- **PsInfo (PsTools)** sistem vasitəsi məsafədə olan sistem haqqında məlumat toplamağa imkan verir (şəkil 7.7). İstifadə qaydası aşağıda göstərilən kimidir:

psinfo [\\kompüter [kompüter [...]] @ f i l e [-u istifadəçinin adı [-p parol]]] [-h] [-s] [-d] [-c]

burada:

\\ **kompüter** – məlumat alınması nəzərdə tutulan kompüterin adı;

Əgər * işarəni göstərsək, onda əmr cari domenin bütün kompüterləri üçün yerinə yetiriləcək;

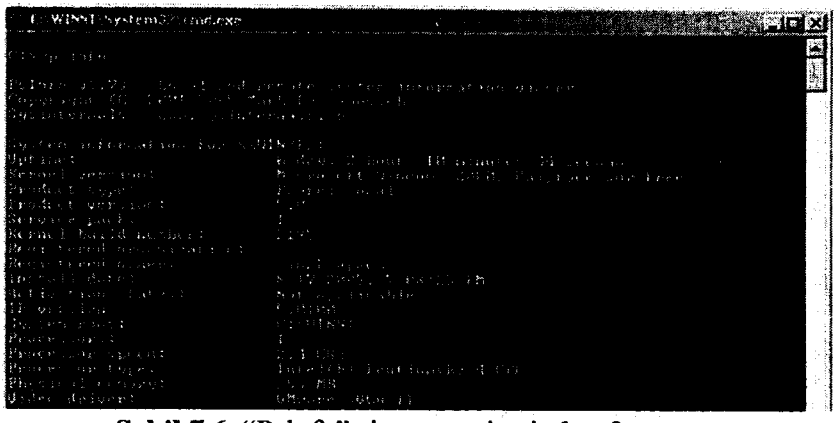
@fiie – məlumat alınması nəzərdə tutulan kompüterlərin siyahısı olan fayl;

-u – məsafədə olan kompüterin sisteminə daxil olmaq üçün istifadəçinin adını təyin edir;

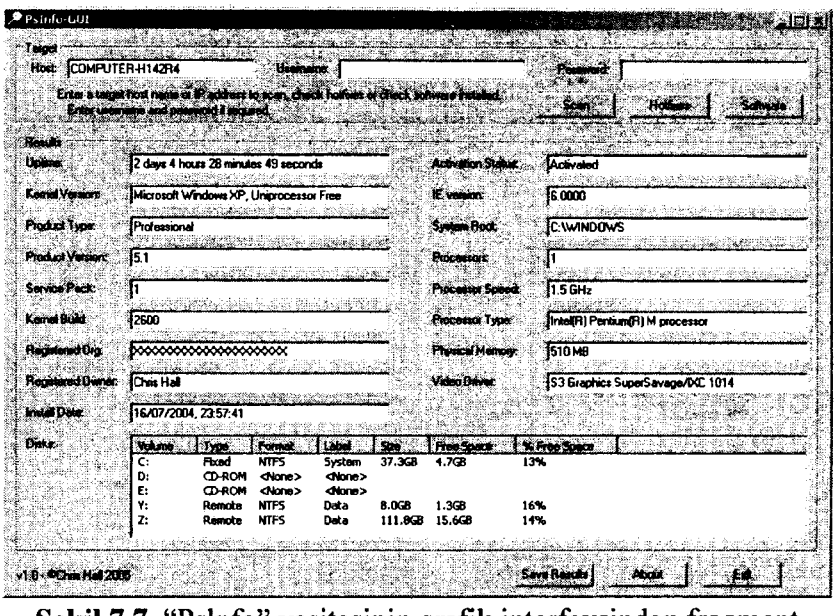
-p – istifadəçinin adı üçün parol təyin edir;

-h – quraşdırılmış yeniləşmələri göstərir;

-s – quraşdırılmış proqram təminatlarını göstərir;
-d – disklər haqqında məlumatı göstərir;
-c – CSV (Comma Separated Value - vergüllə ayrılmış verilənlər) fayl formatında məlumatları hazırlayır.

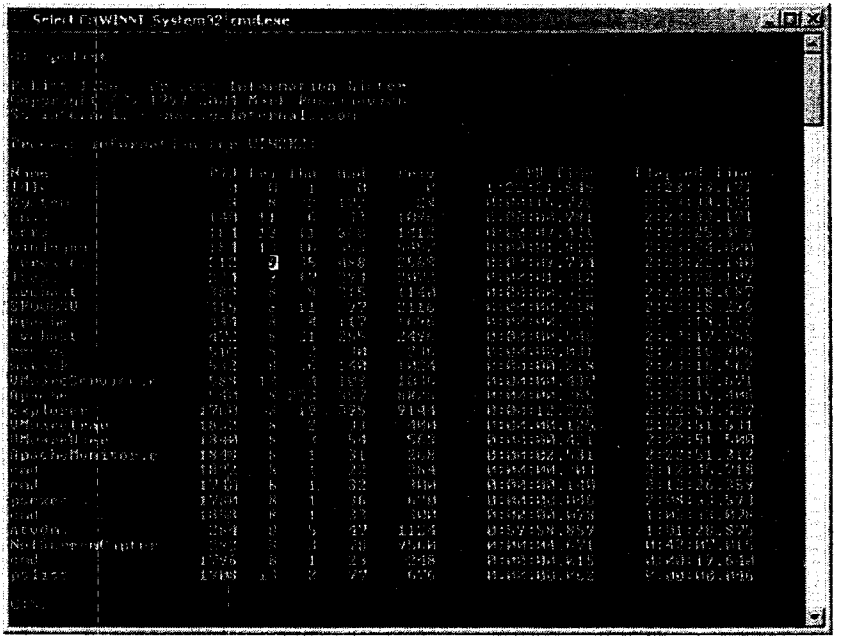


Şəkil 7.6 "Pslnfo" sistem vasitəsindən fraqment



Şəkil 7.7 "Pslnfo" vasitəsinin qrafik interfeysindən fraqment

- **PsList (PsTools)** sistem vasitəsinin köməyi ilə məsafədə yerləşən kompüterdə baş verən proseslərin və yaddaşın istifadə olunması haqqında məlumatların kəsilməz statistikasını almaq mümkündür (şəkil 7.8).



Şəkil 7.8 "PsList" sistem vasitəsindən fraqment

Bu statistikanın yenilənməsi tezliyini saniyələrlə təyin etmək olar. "PsList" sistem vasitənin istifadə qaydaları aşağıdakı kimidir:

pslist [-d] [-m] [- x] [- t] [- s [n] [-r n] [\\kompüter [-u istifadəçinin_adı] [-p parol]] [[-e] prosesin_adı | prosesin identifikatoru]

burada:

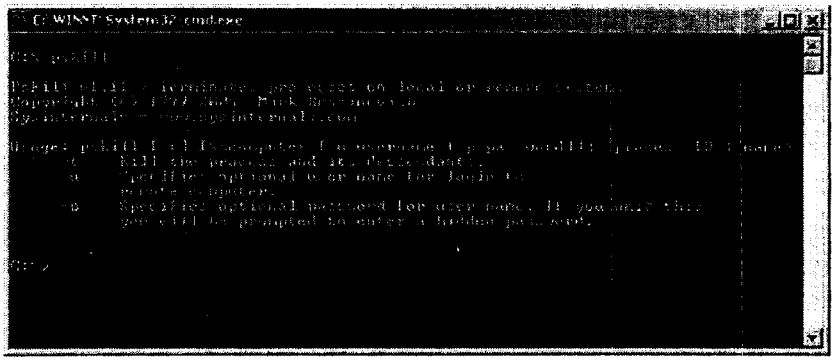
-d – bütün aktiv axınlar üçün statistikanı göstərir;

-m – yaddaşın işlənməsi haqqında məlumatı göstərir;

-x – hər bir prosesin yaddaşı istifadə etmək haqqında məlumatı göstərir;

-t – proseslər ağacını göstərir;
-s [n] – proqram "n" saniyədən sonra yerinə yetirilsin;
-r n – proses bitdikdən sonra onu yenidən işə salmaq;
-u – məsafədə olan kompüterin sisteminə daxil olmaq üçün istifadəçinin adı;
-p – istifadəçinin adı üçün parol.

- **PsKill (PsTools)** sistem vasitəsi məsafədə olan kompüterdə baş verən prosesləri ləğv etmək üçün nəzərdə tutulub (şəkil 7.9).



Şəkil 7.9 "PsKill" sistem vasitəsindən fraqment

İstifadə qaydaları aşağıdakı kimidir:
pskill [\\kompüter [-u istifadəçini_adı] [-p parol]]
<prosesin adı | prosesin_identifikatoru>
"Support Tools" alətləri tərkibində olan digər iki sistem vasitəsinin demək olar ki, çox oxşar cəhətləri vardır. Bunlar "Tlist.exe" və "Kill.exe" sistem vasitələridir. Lakin bunlar tam olaraq eyni deyillər, çünki "Tlist.exe" və "Kill.exe" sistem vasitələri yalnız lokal olaraq işləyirlər.

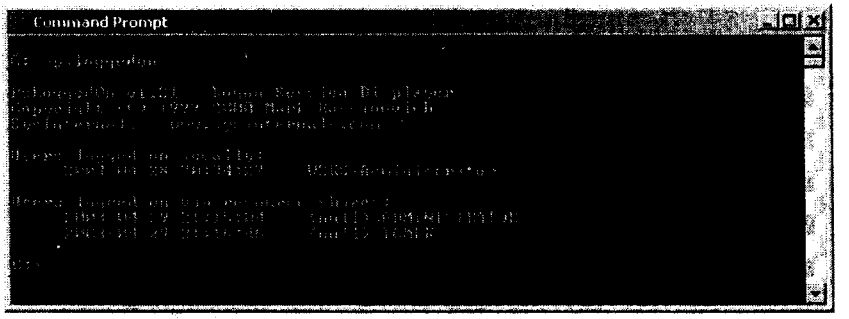
- **PsLoggedOn (PsTools)** sistem vasitəsi hal-hazırda serverə qoşulmuş istifadəçilərin qeydiyyat yazılarının adlarını görməyə imkan verir (şəkil 7.10). İstifadə qaydaları aşağıdakı kimidir:

psloggedon [-l] [-x] [\\kompüter]

burada:

-l – ancaq lokal istifadəçiləri göstərmək;

-x – qoşulma vaxtını göstərməmək.



Şəkil 7.10 "PsLoggedOn" sistem vasitəsindən fraqment

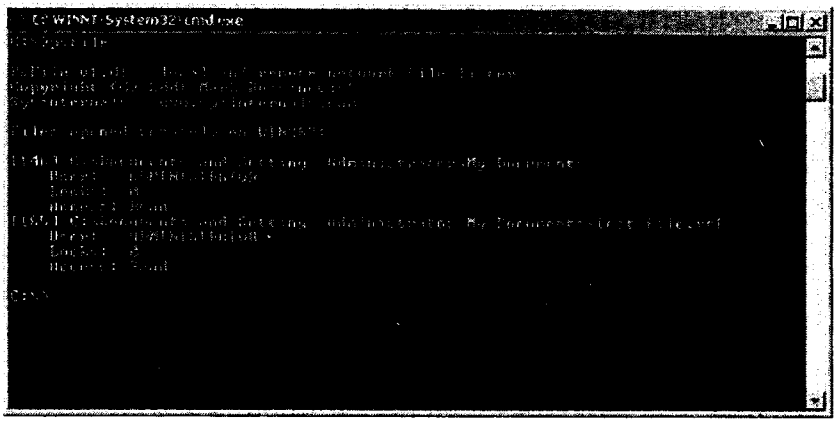
- **PsGetSid (PsTools)** sistem vasitəsinin köməyi ilə işçi stansiyanın və məxsus olduğu domenin mühafizəsi identifikatorunu (SID - *Security IDentifier*) öyrənmək mümkündür (şəkil 7.11). İstifadə qaydaları aşağıdakı kimidir

psgetsid [\\kompüter [,kompüter [,...] | @file] [-u istifadəçini_adı [-p parol]]] [hesab identifikatoru|SID]

Şəkil 7.11 "PsGetSid" sistem vasitəsindən fraqment

- **PsFile (PsTools)** sistem vasitəsinin köməyi ilə giriş əldə edilməsi və istifadəsi vacib olan işçi stansiyada məsafədən hansı faylların istifadə olunduğunu görmək mümkündür (şəkil 7.12). İstifadə qaydaları aşağıdakı kimidir

psfile [\\Məsafədə yerləşən işçi stansiya [-u İstifadəçinin adı [-p Parol]]] [[Id | Tam ünvan] [-c]]



Şəkil 7.12 "PsFile" sistem vasitəsindən fraqment

Bütün bu sadaladığımız sistem vasitələri və komanda sətri ilə işləmək rahat olsun deyə, onların hamısını bir qovluğa yerləşdirmək məqsədəuyğun olardı. Komanda sətrinin icra olunan faylının xassələrində məhz bu qovluğun əməliyyat sistemdə olan tam ünvanını göstərmək lazımdır ki, iş prosesində bu fayllarla bağlı heç bir problem meydana çıxmasın.

7.8 Korporativ şəbəkənin funksionallığı

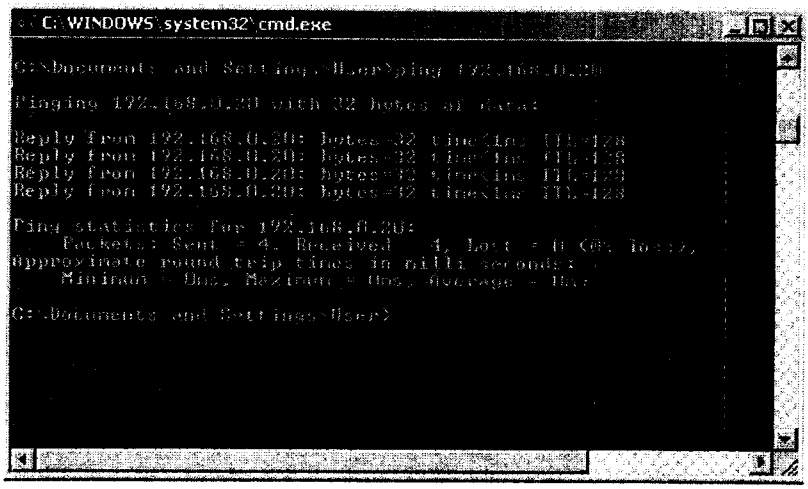
Yuxarıda sadalanan sistem vasitələr, məsafədə olan işçi stansiya haqqında məlumat almağa və bəzi əməliyyatları həyata keçirməyə imkan verirlər. Lakin korporativ şəbəkənin administratoru yalnız bununla kifayətlənməməlidir, o həm də ümumiyyətlə şəbəkənin

işləmə keyfiyyəti ilə müntəzəm olaraq maraqlanmalıdır. Korporativ şəbəkənin işləmə keyfiyyəti bu şəbəkəyə məxsus işçi stansiyaların arasında olan əlaqələrin keyfiyyətli olmasından və lazımlı resursların əlçatan olmasından birbaşa asılıdır. Korporativ şəbəkələrin işinin keyfiyyətinə nəzarət etmək üçün bir sıra proqram və sistem vasitələri mövcuddur.

Ping. Bu silsilədən olan və ən sadə sayılan proqramlardan biri "ping" (C:\windows\system32\ping.exe) vasitəsidir. Bu proqramın sistem qovluqda yerləşməsi, onu işçi stansiyanın ixtiyari qovluğunda işə salmaq imkanını verir. Bu əmr MS Windows ailəsinin bütün əməliyyat sistemində realizə olunub. Bu əmrin əsas xüsusiyyətlərindən biri ondan ibarətdir ki, onun parametrlərinin siyahısı sistemdən asılı olaraq müxtəlif ola bilər, lakin əsas funksiyaları isə dəyişilməz olaraq qalır. Şəkil 7.13-də "ping 192.198.0.20" əmrinin komanda sətri pəncərəsində və ya MS DOS əməliyyat sistemi rejimində yerinə yetirilməsi funksiyasının nəticəsi göstərilmişdir. Bu əmr şəbəkənin aşağıda sadalanan parametrlərini təyin etməyə imkan verir:

- şəbəkədə kompüterin əlçatan olması;
- tələb olunan kompüterlə məsafədə olan kompüter arasında kabel xəttinin işləmək qabiliyyətini;
- kompüterlər arası əlaqənin keyfiyyətini.

Əgər şəbəkənin kabel xəttinin yanından yüksək gərginliyə malik kabellər keçərsə, onda orada yaranan maqnit sahəsi nəticəsində şəbəkə kabelinin işinə xələl gəlmiş olar. Bəzən korporativ şəbəkələrin elə seqmentləri olur ki, orada aşağı ötürülmə sürəti tələb olunur. Belə olan halda adi hab (hub) qurğusu, 100 Mbit/s sürəti dəstəkləyən kommutator qurğusu ilə əvəz edilir. Real praktikada bunun bir neçə səbəbi var, lazım gəldikdə kommutatorun portlarını daha aşağı sürətə sazlayaraq şəbəkənin əvvəlki və ya tələb olunan ötürmə qabiliyyətini əldə etmək olar.



Şəkil 7.13 "ping 192.168.0.20" əmrinin yerinə yetirilməsi

Ipconfig - bu əmr yerinə yetirildiyi kompüterin şəbəkə parametrlərini müəyyən etməyə kömək edir. Aşağıda MS Windows əməliyyat sistemi ailəsinin ixtiyari versiyasında bu əmrin "all" parametri ilə yerinə yetirilməsi göstərilmişdir (şəkil 7.14). Bundan başqa "ipconfig" əmrinin aşağıda sadalanan parametrlərlə də istifadə etmək mümkündür:

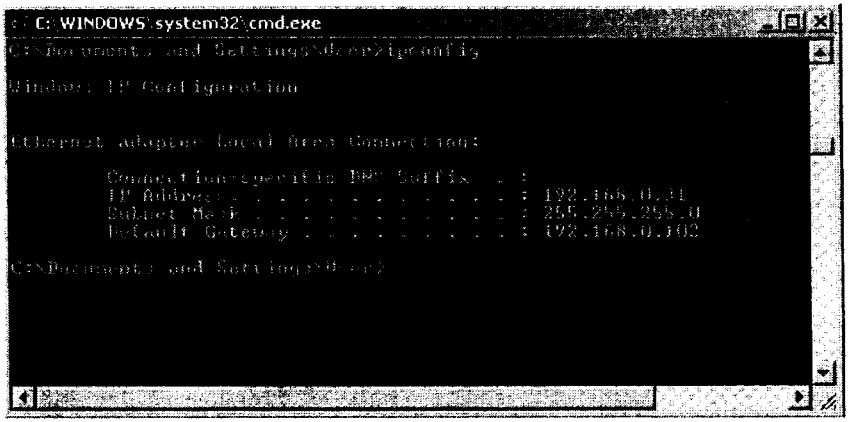
- renew [adapter]
- release [adapter]
- flushdns
- displaydns
- registerdns
- showclassid adapter
- setcalssid adapter [classid]

buradada adapter – qoşulmanın adı deməkdir.

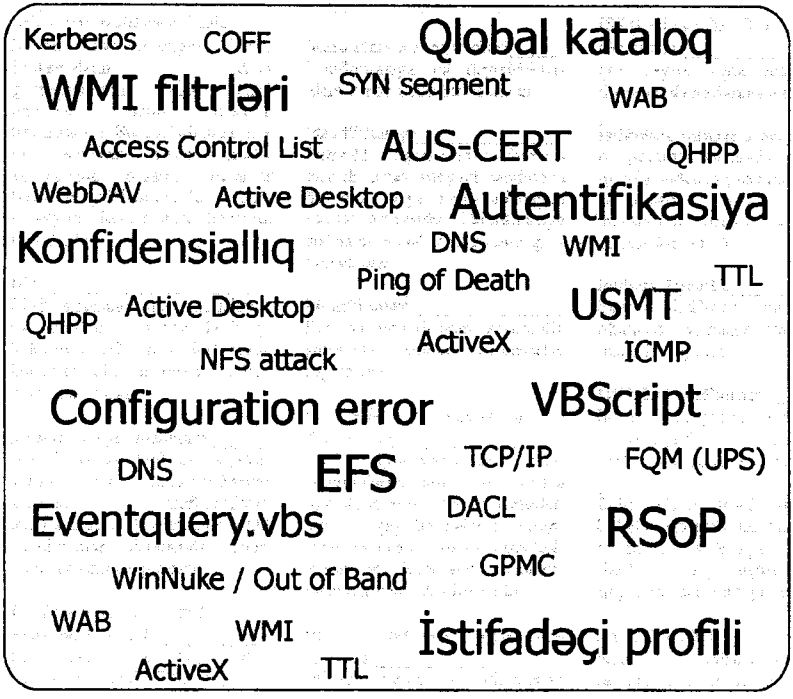
Şəkil 7.15-də göstərildiyi kimi, heç bir parametr daxil etmədikdə "ipconfig" əmri, yalnız əmr yerinə yetirildiyi kompüterin IP ünvanı haqqında məlumat verəcək. Korporativ

şəbəkədə işçi stansiyaların quraşdırılması zamanı meydana gələn çatışmazlıqları yoxlamaq üçün bu əmri istifadə etmək olar.
Məsafədə olan kompüterdə komanda sətri proqramının yerinə yetirilməsi üçün lazımi vasitələr olduqda, bu əmri məsafədə olan işçi stansiyanın və ya serverin sazlanma parametrlərinin yoxlanılması üçün də tətbiq etmək olar.

Şəkil 7.14 "ipconfig/all" əmrinin yerinə yetirilməsi



Şəkil 7.15 "ipconfig" əmrinin yerinə yetirilməsi



Kitabda istifadə olunan terminlərin

İZAHLI LÜĞƏTİ

İZAHLI LÜĞƏTİ

ACL – *Access Control List*
MS Window Server 2003 və 2000 Server əməliyyat sistemlərinə məxsus olan, obyektə təhkim olunmuş icazələr siyahısı.

Active Desktop
Üzərinə aktiv tərkibli elementlərin əlavə olunmasına imkan verən iş masası.

Active Directory
Windows platformasının mərkəzi komponenti olan kataloqlar xidməti - obyektlərin və şəbəkə mühitinin qarşılıqlı əlaqələrinin idarə olunması üçün vasitədir.

ActiveX
Eyni zamanda bir neçə müxtəlif təyinatlı proqram tərəfindən verilənlərin müştərək istifadəsinin vahid qaydalar toplusudur.

ADE – *Application Deployment Editor*
Adi hüquqlara malik istifadəçi korporativ şəbəkəyə daxil olan zaman onun üçün əvvəlcədən administrator tərəfindən təyin olunan proqram təminatlarının tam quraşdırılmasına imkan verən vasitə.

Administrativ şablonlar
Əməliyyat sisteminin daxilində olan standart idarəetmə siyasətinin qaydalar toplusudur və yalnız administrator hüquqlu istifadəçilər üçün nəzərdə tutulub.

ADMT – *Active Directory Migration Tool*
İlkin domendən istifadəçiləri, kompüter obyektlərini, qrupları və kataloqlar xidmətinin digər obyektlərini başqa domenə keçirilməsi xidməti.

ADSI – *Active Directory Services Interface*
Kataloqlar xidmətinə müraciət üçün istifadə olunan interfeys.

Adware – *Reklam təyinatlı proqramlar*
Proqram təminatının yayılma modelidir. Əsas ideya ondan ibarətdir ki, proqram istehsalçısı ödənişi son istifadəçidən deyil, reklam yerləşdirən şirkətdən qəbul edir.

Anonymous FTP abuse
Anonim girişə icazə verən FTP serverlərə yönələn hücum növü.

API – *Application Programming Interface*
Proqram vasitələrini proqramlaşdırma interfeysi.

Applet
Java proqramlaşdırma dilində yazılan və veb səhifəyə əlavə kimi daxil edilməsi nəzərdə tutulan proqramdır.

AusCERT
Korporativ şəbəkələrdə informasiya təhlükəsizliyinin pozulmalarının qeydiyyatını aparan təşkilat.

Autentifikasiya
Unikal məlumat əsasında subyektin təqdimatından sonra onun həqiqiliyinin yoxlanılması prosedurudur. Ən sadə misal kimi ad və parolu göstərmək olar.

Avtorizasiya
Girişə məhdudiyyəti olan müxtəlif sistemlərdə tələb olunan parametrlərin yoxlanılması və bundan sonra istifadəçiyə müəyyən olunmuş hüquqların təyin olunması prosesidir.

Bədəməl şəxs (*bədəfkar*)
Kompüter şəbəkələrində olan boşluqların, zəif nöqtələrin axtarışı və özgə şəbəkələrinə məqsədli şəkildə ziyan vurmaqla məşğul olan şəxs.

Break-in
Sistemdə realizə olunan müxtəlif təhlükəsizlik servislərinin dayanmasına gətirib çıxaran hücumlar.

CERT/CC – *Computer Emergency Response Team / Coordination Center*
Kompüter insidentlərinin həllinə kömək komandası.

CGI – skriptlər
Common Gateway Interface
Kliyent-server modelinin şlyuz interfeysinin qaydalarına riayət edən və serverdə yerinə yetirilən proqramdır.

Citrix MetaFrame
Bu proqram vasitəsi istifadəçiyə eyni serverdə bir seans çərçivəsində bir neçə dərc olunmuş proqramları işə salmaq imkanını verir.

Cmd
Əmrləri yerinə yetirmək üçün komanda sətri vasitəsi.

COFF – *Common Object File Format*
Obyekt fayllarının ümumi formatı

COM – *Component Object Model*
Microsoft korporasiyası tərəfindən təklif olunan texnoloji standart. Qarşılıqlı əlaqədə olan paylanmış komponentlər əsasında

proqram təminatı yaratmaq üçün nəzərdə tutulub və hər bir element eyni zamanda (paralel) müxtəlif proqramlarda istifadə oluna bilər.

Commercial Software
Kommersiya tipli proqramlar, yaradılmış məhsuldan mənfəət əldə etmək və yayılması üçün müəyyən mükafatlar sistemini özündə cəmləşdirir.

Computer Management
Yalnız lokal kompüteri deyil, həm də məsafədə yerləşən kompüteri idarə etmək üçün istifadə olunan və MS Windows əməliyyat sisteminin daxilində olan sistem vasitə.

Configuration error
İntensiv istifadə olunan proqramlarda istifadəçilərin düzgün konfiqurasiya olunmaması nəticəsində meydana çıxan boşluqlar.

Configure Your Server
MS Windows Server 2003 əməliyyat sistemində serveri konfiqurasiya etmək üçün proqram vasitəsi.

Cracked password
Kompüter şəbəkələrində asan tanına bilən parolların müəyyən olunmasına yönələn hücum növü.

CSIRT – *Computer Security Incident Response Teams*
Kompüter şəbəkələrində təhlükəsizlik insidentlərinin həllinə kömək komandası.

CSMA/CD - *Carrier Sense Multiple Access / Collision Detection*
Ethernet şəbəkələrində kolliziyaları təyin etmə ilə verilənlərin mübadiləsi mühitinə giriş metodu

Çoxdəyişənli reqressiya
Bir neçə asılı olmayan dəyişənlə, asılı olan dəyişən arasında əlaqəni analiz etməyə imkan verən model.

Çoxünvanlı qayda – *multihomed*
Çoxünvanlı qayda korporativ şəbəkənin bir şəbəkə interfeysinə tətbiq olunduqdan sonra digər şəbəkə interfeysləri üçün yeni əlaqələr qurur.

DACL – *Discretionary Access Control List*
Girişə diskresion nəzarət siyahısı – Etibar edilən subyektin mühafizə olunan obyektə giriş imkanının olub-olmadığını müəyyən edən siyahı.

Dataqram
Şəbəkədə müstəqil şəkildə ötürülə bilən paket.

Demoware
Proqram təminatının yayılma modelidir. Proqramda funksional məhdudiyyətlərin mövcud olduğu hal. Əsasən proqram vasitəsini tanıtmaq üçün istifadə olunur və pulsuz şəkildə yayılır.

Dəstəklənən autentifikasiya
Digər meşədə, məsafədə yerləşən serverdə autentifikasiyanın dəstəklənməsi metodları. Məsələn, Kerberos və NTLM şəbəkə qeydiyyatı, NTLM interaktiv qeydiyyatları, istifadəçinin məxsus olmadığı meşədə fiziki qeydiyyatı, digər meşələrdə çoxsəviyyəli proqram təminatlarının Kerberos nümayəndələrinə ayırması.

DFS – *Distributed File System*
Kompüter şəbəkələrində disk resurslarının birgə istifadəsinin idarə olunması məsələsini asanlaşdırmaq üçün nəzərdə tutulub.

DHCP – *Dynamic Host Configuration Protocol*
Hostun dinamik konfiqurasiyası protokolu olan – RFC 1541 əsasında şəbəkə standartı. İstifadəçi kompüterlərinə server tərəfindən IP ünvanlarının və digər konfiqurasiya məlumatlarının təhkim olunmasını reqlament edir.

DLL – *Dynamic Link Library*
MS Windows əməliyyat sistemləri ailəsində istifadə olunan dinamik qoşulan kitab-xanalar.

DNS – *Domain Name System*
Domenin adlar xidməti – mətnlə yazılmış ünvanların (domen adları) rəqəmli IP ünvanlarına çevirən texnologiya

DNS poisoning
DNS–serverlərin ardıcıllığını əvvəlcədən müəyyən edilməklə domen adlarının rekursiv sorğulardan istifadə etməsi.

Domen
Vahid mərkəzi istifadəçi bazası, vahid qrup və lokal siyasəti, vahid təhlükəsizlik parametrləri olan və bir şəbəkəyə məxsus kompüterlər qrupudur.

Domen kontrolleri
Korporativ şəbəkə daxilində vahid istifadəçi bazası, qrup və lokal siyasəti, təhlükəsizlik parametrləri olan vahid bir mərkəzdir.

Domenin verilənləri
Domen daxilində yerləşən obyektlər haqqında məlumatdır.

DoS – *Denial of Service*
Bu halda bədəməl şəxs informasiyanı əldə etməyə deyil, o

yalnız informasiyanı sahibi üçün əlçatmaz etməyə çalışır.

EFS – *Encrypting File System*
Faylları sistemə fiziki giriş ə ldə etmiş digər şəxslərdən mühafizə etmək məqsədi ilə şifrləmə sistemi.

Email bombardment
Əvvəlcədən seçilmiş bir elektron ünvana müxtəlif elektron ünvanlardan külli miqdarda məktubların göndərilməsi.

Email spoofing
Başqa subyekt adından elektron məktubun göndərilməsi yolu ilə müxtəlif hücüm strategiyasının qurulması

EMS – *Emergency Management Services*
Server şəbəkədən əlyetən olmadıqda administratora məsafədən idarəetmə, bərpa işləri və bir sıra şəbəkə idarəçiliyinə aid olan proseduraları yerinə yetirmək imkanını yaradan vasitədir.

Enterprise UDDI *(Universal Description, Discovery and Integration)*
XML veb-servisləri üçün dinamik və çevik infrastruktur.

Error Messages for Windows
Əməliyyat sistemində olan çatışmazlıqları müəyyən edən əlavə sistem vasitəsi.

ESA –
Expert Sniffer Analyzer
Protokolların analizatoru.

ESB –
External Security Bulletin
CERT təşkilatları tərəfindən dərc olunan xarici təhlükəsizlik bülleteni.

Ethernet şəbəkəsi
Xerox korporasiyası tərəfindən təklif olunan şəbəkə tipi. Ethernet şəbəkəsinin işləmə prinsipi bu şəbəkəyə məxsus şəbəkə kartlarının çıxışlarını paralel olaraq qoşulmasından ibarətdir.

Etibarlılıq
Verilmiş zaman kəsiyində sistemin əvvəlcədən müəyyən olunmuş reqlamentə görə sapmalarsız və dayanmadan iş-ləməsi halı.

Event Viewer
MS Windows əməliyyat sistemləri ailəsində sistem jurnallarına baxmaq üçün nəzərdə tutulmuş proqram vasitəsi.

Eventquery.vbs
Bu komanda sətri aləti proqram təminatlarına məxsus lokal jurnalların bütün məlumatlarını ekrana çıxarmağa imkan verən vasitədir.

Əlyetənlik
Avtorizə edilmiş istifadəçilərin istədiyi zaman informasiyanı əldə etmək imkanı.

Əməliyyat sistemi
Kompüterin aparat vasitələrini, fayl sistemini, verilənlərin giriş/çıxış sistemini və tətbiqi proqramların yerinə yetirilməsinə imkan yaradan baza kompleksi.

Failover
Sistem sapmaları.

FIN - *sonuncu bit*
Şəbəkələrdə bağlantının bitməsini göstərir.

FCM (UPS - *Uninterruptible Power Supply*)
Fasiləsiz Cərəyan Mənbəyi.

Freeware
İsitfadəsi üçün heç bir ödəniş tələb olunmayan proqram təminatının yayılma modelidir.

FRS –
File Replication Service
Seçilmiş serverlər arasında faylların təyin olunmuş kataloqda çoxtərəfli replikasiyasını dəstəkləyən xidmət.

FTP –
File Transfer Protocol
Faylların Ötürülmə Protokolu.

Giriş dərəcəsi
İstifadəçinin şəbəkə resurslarından istifadə etmək hüququnu təyin edir.

GPM –
Group Policy Modeling
Qrup siyasətinin modelləşdirilməsi – bu vasitə ssenariləri təyin edir və onlar üçün siyasətin qaydalarına, proqramlarına və təhlükəsizliyinə baxış keçirmə imkanı verir.

GPMC – *Group Policy Management Console*
Qrup siyasətinin idarəetmə konsolu – MS Windows Server 2003 əməliyyat sisteminə əlavə genişlənmə kimi təklif olunur və qrup siyasətinin elementlərini idarə etmək üçün nəzərdə tutulub.

GPO –
Group Policy Object
Qrup siyasətinin obyekti – Active Directory xidmətində işçi stansiyaların və məsafədən qoşulan istifadəçilərin konfiqurasiyalarının mərkəzləşdirilmiş şəkildə idarə edilməsindən ibarətdir.

GUID - *Globally Unique Identifier*
Dəyişdirilmiş domenin identifikasiyasının qlobal unikal identifikator vasitəsi ilə həyata keçirilməsidir.

HTML - *HyperText Markup Language*
İnternetdə sənədlərin səhifələnməsinin standart dilidir.

XML – *Extensible Markup Language*
Səhifələnmənin genişləndirilmiş dili – proqramlar arasında məlumatların mübadiləsi zamanı strukturlaşdırılmış verilənlərin saxlanılması üçün nəzərdə tutulmuşdur.

IAT – *Import Address Table*
İdxal cədvəlləri, idxal olunan funksiyaların bütün göstəricilərinin dəqiq daxil olunması üçün nəzərdə tutulmuşdur. Bu göstəricilərin hər biri sistemin xarici kitabxanalarında onların ünvanlar fəzasına yükləndikdən sonra müəyyən funksiyanın ünvanını təmsil edir.

ICA - *Independent Computing Architecture*
Citrix sistemləri əsasında işləyən və WinFrame vasitəsi ilə birgə Windows NT serverini mini-kompüter kimi işlətməyə imkan verən texnologiya.

İcazələr siyasəti
Administrator tərəfindən istifadəçilər üçün təyin olunan resurslara giriş qaydaları toplusudur.

İcazələrin uyğunlaşması
MS Windows 2000 Server əməliyyat sistemindən və ya Terminal Server 4.0 vasitəsindən olan istifadəçilərin icazələrinin MS Windows Server 2003 əməliyyat sistemində işinin tənzim olunması prosesi.

ICMP – *Internet Control Message Protocol*
İnternet şəbəkəsinin əsas protokollarındandır. Əsas məqsədi şəbəkədə yerləşən işçi stansiyanın əməliyyat sistemi tərəfindən şəbəkə xidmətlərində baş verən səhvlər və ya qüsurlar haqqında məlumatların əks etdirməsindən ibarətdir.

İdarəetmə mexanizmləri
Müxtəlif əməliyyat sistemlərində fərqli konfiqurasiya elementlərini və dəyişiklikləri idarə etmək üçün bir vasitədir.

İdentifikasiya
Subyekti digərlərindən fərqləndirmək üçün subyekt tərəfindən öz adını və ya nömrəsini bəyan etməsi prosesidir. İdentifikasiya sisteminə misal kimi ştrix-kodları gös-tərmək olar.

İdentifikator
Hər bir istifadəçini korporativ şəbəkədə tanıdan parametrlər toplusudur.

IETF – *Internet Engineering Task Force*
1986-cı ildə yaradılan, layihəçilərin, alimlərin, şəbəkə operatorlarının və provayderlərin açıq beynəlxalq birliyi. Əsas məqsədi şəbəkə protokollarının və İnternetin arxitekturasının inkişaf etdirilməsidir.

IIS – *Internet Information Services*
Micrisoft korporasiyası tərəfindən təklif olunan İnternet informasiya servisləri toplusudur.

İnformasiya təhlükəsizliyi
İnformasiya təhlükəsizliyi informasiyanın emalı, saxlanılması və ötürülməsi zamanı onun konfidensiallıq, tamlıq və əlyetənlik kimi xassələrinin təmin olunmasıdır.

Intruder gained root access
Bədəməl şəxsin sistemə adi istifadəçi hüququnda daxil olub sonra isə administrator hüququ almağa nail olmasıdır.

Intruder installed packed sniffer
Sistemdə xüsusi ələ keçirmə proqramı yerləşdirməklə sistemi hücumlara açıq edən vasitə.

Intruder installed Trojan horse program
Sistemə daxil olan bədəməl şəxs, orada özünə məxsus olan cəsus proqramını yerləşdirir və onun köməkliyi ilə sistemə təkrar daxil olmağı asanlaşdırır.

IP spoofing
İxtiyari şəbəkədə IP ünvanın dəyişdirilməsi (əvəz olunması) vasitəsi ilə reallaşan hücum tipləri.

IPSec – *IP Security*
IETF təşkilatı tərəfindən təyin olunan IP protokolu əsasında işləyən şəbəkələrdə informasiya ötürülməsinin etibarlı/konfidensial standartıdır. IPSec ən çox virtual məxsusi şəbəkələrdə istifadə olunur.

ISN – *Initial Sequence Number*
Əlaqə yaratma prosesində (TCP/IP protokolunda) ilkin ardıcıllığın nömrələri

ISTG – *Inter Site Topology Generator*
Çoxsaylı sayta malik olan domenin dəstəklənməsi alqoritmi.

İstifadəçi parametrləri
Korporativ şəbəkədə istifadəçi qeydiyyatdan keçən zaman sistem tərəfindən qəbul edilən məlumatlar (parol, ad, və s.).

İstifadəçi profili
Şəxsən istifadəçi üçün təyin olunmuş qaydalar və texniki

imkanlar toplusu.

İstifadəçi verilənləri
İstifadəçinin şəbəkə serverlərində yerləşdirdiyi və yalnız onun profilinə uyğun məlumatlar.

İstifadəçinin adı – *Login*
Şəbəkə xidmətlərini təklif edən tərəfdən istifadəçiyə şəbəkəyə daxil olmaq üçün keçdiyi qeydiyyat zamanı təyin olunan ad.

JANET-CERT
Kompüter şəbəkələrində informasiya təhlükəsizliyinin pozulmalarının qeydiyyatını aparan təşkilat.

JavaScript language
İstifadəçilərin veb saytlarla qarşılıqlı əlaqəsini yaradan ssenarilərin proqramlaşdırma dili.

Kataloqun topologiyası
Bütün domenlərin siyahısı və qlobal kataloqların toplusudur.

Kerberos
Real rejimdə məlumatları bir nöqtədən digər nöqtəyə ötürülmə zamanı şəbəkə kommunikasiyalarının şifrələməsini dəstəklə-yən proqram vasitəsi.

Kerberos Domain Controller
Domen daxilində autentifikasiya mexanizmidir.

Keş yaddaş
Daha çox istifadə olunması ehtimal olunan məlumatları saxlayan çevik əlaqəli aralıq bufer.

Klaster
(8 bəndə qədər)
Bu xidmət yalnız MS Windows Server 2003 əməliyyat sisteminin Enterprise Edition və Datacenter Edition versiyalarında mövcuddur. Verilənlər bazası, elektron poçt sistemi, fayl serverləri və çap serverləri kimi kritik proqram vasitələri üçün yüksək hazırlıq və miqyaslılıq xidmətlərini yerinə yetirir.

Komanda prosessoru
İstifadəçilərin əməliyyat sis-temi ilə qarşılıqlı əlaqəsini təmin edən ayrıca proqram.

Kommutator
Ötürülən paketlərin komutasiyası üçün nəzərdə tutulmuş proqram və ya qurğu.

Konfidensiallıq
İnformasiyanın yalnız müəyyən olunmuş şəxslərə əlçatan olmasıdır.

Korporativ şəbəkənin funksionallığı
Vahid zaman anında informasiya paketlərinin axını və məlumatların ötürülmə sürəti ilə təyin olunur.

Kross-sertifikatlaşdırma
Bu vasitənin köməyi ilə qlobal şəbəkələrdə sertifikatların qarşılıqlı yoxlanılması prosesi həyata keçirilir.

Qeyri-səlis çoxluqlar
Klassik çoxluqlar nəzəriyyəsinin genişlənməsidir və qeyri-səlis məntiqdə istifadə olunur. Qeyri-səlis çoxluqlar mənsubiyyət funksiyası ilə xarakterizə olunurlar hansı ki, müəyyən çoxluğu (qeyri-səlis çoxluğun daşıyıcısı olan) [0; 1] parçasında əks etdirir. Mənsubiyyət funksiyasının qiyməti, müvafiq daşıyıcı elementin qeyri-səlis çoxluqlara mənsubiyyətlik dərəcəsini göstərir. Bu qiymət 0-dan (tam qeyri-mənsubiyyətlik) 1-ə (tam mənsubiyyətlik) qədər dəyişə bilər.

Qeyri-səlis ədədlər
Normal və qabarıq mənsubiyyət funksiyası olan, həqiqi ədədlərin universal çoxluğunun qeyri-səlis alt çoxluğudur. Yəni: a) aparıcının elə bir qiyməti var ki, orada mənsubiyyət funksiyası birə bərabərdir; b) öz maksimumundan sola və ya sağa kənarlaşanda mənsubiyyət funk-siyası artmır.

QHPP
Qeyri-Həmcins Puasson Prosesi.

Qlobal kataloq
Active Directory vasitəsinin bütün obyektlərinin ehtiyat nüsxələri saxlanılan domen kontrolleridir.

Qonaq – *Guest*
Şəbəkə resurslarından istifadə hüququ məhdudlaşdırılmış istifadəçi.

QoS – *Quality of Service*
Xidmətin keyfiyyəti.

Qovluğun yönəldilməsi
Köhnə mühitdən olan istifadəçi qovluqlarının yeni mühitə tam uyğunlaşdırılması texnologiyası.

Qrup siyasəti
Korporativ şəbəkə çərçivəsində istifadəçilərin və kompüterlərin administrativ nəzarətini həyata keçirməyə imkan verir.

Qrup siyasətinin redaktoru
Group Policy Editor
Qrup siyasətinin qaydalarını dəyişdirmək üçün istifadə olunan vasitə.

Land/Latierка
Bəzi əməliyyat sistemində TCP/IP stekinin reallaşmasında boşluqlardan istifadə etmək və əsas məramı kompüterin acıq portuna SYN bayrağı qeyd olunan yalançı TCP-paketlərini göndərməkdən ibarətdir.

LDAP – *Lightweight Directory Access Protocol*
Məlumat kitabçalarına giriş əldə etmək üçün protokollar toplusu.

LE – *Linear Executable*
OS/2 əməliyyat sistemində xətti icra olunan faylların saxlanılması üçün istifadə olunur.

LX – *Linear eXecutable*
OS/2 əməliyyat sistemində xətti icra olunan faylların saxlanılması üçün istifadə olunur.

Log fayl
Əməliyyat sistemində baş verən hadisələr haqqında məlumatları xronoloji ardıcıllıqla özündə cəmləyən fayl.

Logon Settings
İstifadəçinin və ya sistemin qeydiyyatı üçün tələb olunan parametrlər toplusu.

Lokal səviyyə
Lokal səviyyə ən çox təhlükəsizlik siyasəti elementləri tətbiq olunan səviyyə sayılır. Onlar məhz server proqramlarının quraşdırıldığı kompüterin təhlükəsizliyini təmin edirlər.

LSA – *Local Security Authority*
MS Windows əməliyyat sistemində təhlükəsizlik siyasətini gücləndirmək üçün nəzərdə tutulub. Bu gücləndirmə istifadəçinin sistemə girişi zamanı giriş markeri yaratmaqla həyata keçirilir.

MAC – *Media Access Control*
Məlumatların ötürülmə mühitinə giriş səviyyəsinin ünvanları - şəbəkə kartına istehsalçı tərəfindən təyin olunmuş 48 bitlik unikal ünvandır.

Manage Your Server
MS Windows Server 2003 əməliyyat sistemini quraşdırandan sonra administrator kimi serverə ilk giriş zamanı ekrana gələn birinci sistem vasitəsi.

MAPI – *Messaging Application Programming Interface*
MS Windows əməliyyat sistemləri ailəsində elektron poçt vasitələri ilə işləyən proqramın interfeysi. MAPI interfeysi elektron poçt qutusunu idarə etmək üçün geniş imkanlar və texniki güclü alətlər təqdim edir.

Miqyaslılıq
Əməliyyat sisteminin oxşar tətbiqi proseslərinin bir və çoxprossesorlu rejimlərdə eyni məharətlə yerinə yetirməsi.

Meşə
Kataloqlar xidmətinin xarici sərhədini təşkil edir.

Meşələrarası etibar münasibətləri – *Forest trust*
Meşələrarası etibar münasibətləri

meşələrin təhlükəsizlik problemlərinin idarə olunmasını asanlaşdırır. Etibar edən meşə istifadəçilərin adlarına məhdudiyyətlər qoymaq hüququna malikdir və bu istifadəçilərin autentifikasiyasını digər meşələrə etibar edir.

Məhsuldarlıq
Verilmiş zaman kəsiyində sistemin əvvəlcədən qarşısına qoyulmuş tələbləri tam şəkildə yerinə yetirməsi halıdır.

Mənsubiyyət funksiyası
Qeyri-səlis çoxluğun mənsubiyyət funksiyası – klassik çoxluqlarda olan indikator funksiyasının ümumiləşdirilməsidir. Qeyri-səlis məntiqdə bu funksiya həqiqətin dərəcəsini müəyyən edir.

Microsoft .NET Framework
Microsoft şirkəti tərəfindən təklif olunan, qarşılıqlı əlaqədə olan proqram vasitələrinin proqramlaşdırma modelidir

Misuse of hosts sources
Host resurslarının düzgün istifadə olunmaması nəticəsində meydana gələn boşluqlar.

MMC – *Microsoft Management Console*
MS Windows Server 2003 əməliyyatlar sistemində konfiqurasiya və ya idarə etmək üçün nəzərdə tutulmuş konsol.

MS ACCESS
Verilənlər bazasının idarəetmə sistemi.

MS Exchange Server
Elektron məktublarının qəbul edilməsini, göndərilməsini və birgə istifadə olunmasını təmin edən Microsoft şirkətinə məxsus proqram təminatıdır.

MSMQ – *Microsoft Message Queuing*
Məlumatların Active Directory vasitəsində olan yollama siyahısına (distribution lists) daxil olunması funksiyası

MUI – *Multilingual User Interface*
MS Windows əməliyyat sistemlərində tətbiq olunan və interfeys tərəfindən digər dillərin dəstəklənməsi xidmətidir.

Multimaster
Active Directory xidmətində çoxtərəfli replikasiya elementi.

Nagware
Proqram təminatının yayılma modelidir. İstifadəçi istifadə etdiyi proqram vasitəsinin tam kommersiya versiyalı proqram olmadığı haqqında müntəzəm olaraq məlumat alır.

NAT – *Network Address Translation*
TCP/IP şəbəkələrində tranzit

paketlərin IP ünvanlarını yenidən formalaşdırmağa imkan verən mexanizmdir.

NetBIOS – *Network Basic Input/Output System*
Kompüter şəbəkəsi vasitəsi ilə proqramların qarşılıqlı əlaqəsi üçün nəzərdə tutulmuş protokol. OSI modelinin seans və nəqliyyat səviyyələrində yerləşir.

Netlogon
Bu vasitə qrup siyasətinin daxili parametrlərini MS Windows Server 2003 əməliyyat sistemində olan kompüterləri sazlamaq üçün istifadə olunur.

NFS attack
(Network File System)
Şəbəkə fayl strukturuna yönələn hücum tipi.

NTLM – *Windows NT LAN Manager*
Windows NT 4.0 əməliyyat sistemində autentifikasiya protokolu.

OEM – *Original Equipment Manufacturer*
Digər şirkətin məhsulunu eyni adla təqdim edən istehsalçı.

OSI – *Open System Interconnection*
Açıq sistemlərin qarşılıqlı əlaqəsinin etalon modeli.

Paralel LDAP qoşulma
İstifadəçilərin autentifikasiyası məqsədi ilə bir qoşulmada bir neçə LDAP qoşulmalarına icazə verilir.

Parolların miqrasiyası
MS Windows NT Server 4.0 əməliyyat sisteminin domenlərindən MS Windows 2000 Server və MS Windows Server 2003 əməliyyat sistemlərinin domenlərinə parolların köçürülməsi prosesi.

PAS - *Partial Attribute Set*
Qlobal kataloqlarla replikasiya olan MS Windows Server 2003 əməliyyat sisteminin domenlərində qlobal kataloqun sinxronlaşdırma vəziyyətinin yadda saxlanılması.

Permissions
İstifadəçiyə şəbəkə daxilində təyin olunan hüquqlar.

Ping əmri
Əvvəlcədən müəyyən olunmuş serverə exo paketlərin ötürülməsini təmin edən komanda sətrinin əmri.

Ping of Death
Hücum edilən qovşağa data-qramların fraqmentlərinin göndərilməsindən ibarətdir.

PKI - *Pulic Key Infrastructure*
Açıq açarlr infrastrukturu.

Plug and Play
Qoşul və işlə
Bu vasitənin köməyi ilə kompüterə yeni plata qoşulduqda və kompüter növbəti dəfə işə salındıqda plata avtomatik olaraq konfiqurasiya olunur.

Plug-in *(Plugins)*
MS Windows əməliyyat sistemləri ailəsi üçün nəzərdə tutulmuş xüsusi təyinatlı əlavələr.

POP3 – *Post Office Protocol Version 3*
İxtiyarı kompüter şəbəkələrinə məxsus poçt serverindən elektron məktubları istifadəçinin işçi stansiyasında qəbul etməsi üçün istifadə olunan şəbəkə protokolu.

Prank
Şəbəkə istifadəçilərinin profilinin düzgün yaradılmaması nəticəsində əmələ gələn zəif yerlərinə hücumlar.

Probe, Scan, Scam
Acıq və istifadə olunan portların skan edilməsi və bu portlar vasitəsi ilə müxtəlif servislərə hücumların reallaşdırılması.

Proqram təminatını məhdudlaşdıran siyasət – *Software restriction policies*
Kompüterdə/şəbəkədə əməliyyatlar sistemi tərəfindən icazəsi olmayan və ya etibarlı olmayan proqram təminatlarının işə salınmasının qarşısını almaq üçün istifadə olunur.

Proqramları nəşretmə ilə quraşdırılması
Proqram çox da əhəmiyyətli olmadığı hallarda nəşr etmə əməliyyatı vasitəsi ilə yüklənmənin həyata keçirilməsi.

Proqramları təyinetmə ilə quraşdırılması
Kompüterə təyin olunmuş proqram təminatlarının kompüter növbəti dəfə işə salınan zaman yüklənməyə başlaması.

Proqram vasitələrinin dəstəklənməsi
Vahid əməliyyat sistemi çərçivəsində bir proqram təminatının digəri ilə birgə qüsursuz işləməsi.

PsExec
Bu sistem/administrativ vasitəsi məsafədə olan işçi stansiyalarda komanda sətri əməliyyatlarını yerinə yetirməyə imkan verir.

PsInfo
Bu sistem/administrativ vasitəsi məsafədə olan sistem haqqında məlumat toplamağa imkan verir.

PsKill
Bu sistem/administrativ vasitəsi məsafədə olan kompüterdə baş verən prosesləri ləğv etmək üçün

nəzərdə tutulub.

PsList
Bu sistem/administrativ vasitəsinin köməyi ilə məsafədə yerləşən kompüterdə baş verən proseslərin və yaddaşın istifadə olunması haqqında məlumatların fasiləsiz statistikasını aparmaq mümkündür.

PsLoggedOn
Bu sistem/administrativ vasitəsi hal-hazırda serverə qoşulmuş istifadəçilərin qeydiyyat yazılarının adlarını görməyə imkan verir.

PsTools
Komanda sətrini tətbiq etməklə məsafədən idarə etmənin imkanlarını genişləndirmək üçün əməliyyatlar sisteminə əlavə yüklənən sistem paket proqramı.

RAS - *Remote Access Service*
Serveri məsafədən idarəetmə xidməti.

RDP –
Reliable Data Protocol
Məsafədən emal və host monitorinq üçün nəzərdə tutulmuş külli miqdarda verilənlərin bir dəfəyə ötürülməsini dəstəkləyən nəqliyyat protokolu.

Remote Desktop
Korporativ şəbəkəyə məxsus MS Windows Server 2003 əməliyyatlar sistemi quraşdırılmış ixtiyari serverin "iş stoluna" məsafədən girişi təmin edən sistem vasitə.

Remote data processing –
Verilənlərin məsafədən emalı
Verilənlərin emalının elə formasıdır ki, burada emal zamanı lazım olan giriş/çıxış əməliyyatları şəbəkə vasitəsi ilə həyata keçirilir.

Replikasiya
Verilənlər bazasının ehtiyyat (ikili) nüsxələrinin idarə olunması və yaradılması prosesi. Həmçinin replikasiya bir sıra məlumatları bir neçə yerdə sinxronlaşdırılmasıdır.

RIS – *Remote Installation Service*
Əməliyyat sistemini uzaqdan sazlamaq üçün məsafədən quraşdırma xidməti.

Rlogin or rsh attack
Məsafədən giriş xidmətində olan boşluqlardan istifadəyə yönələn hücum tipi.

Router
Ərazi baxımından məsafədə yerləşən şəbəkələr arasında əlaqəni ünvanlı şəkildə təmin edən qurğu.

RPC –
Remote Procedure Call
Başqa ünvanlar fəzasından (adətən məsafədə yerləşən

kompüterlərdə) kompüter proqramlarına funksiya və ya prosedura çağırmağa imkan verən texnologiya. Korporativ şəbəkələrdə RPC cağırışlarını yerinə yetirən müxtəlif texnologiyalar mövcuddur: Sun RPC (RFC 1831), Net Remoting, XML RPC, Java RMI.

RSoP – *Resultant Set of Policy*
Microsoft Management Console vasitəsinin daxilində olan xidmətlər toplusu şəklində təklif olunur. İki digər rejimdə (yəni, qeydiyyat və planlaşdırma rejimlərində) olan siyasətin cari qaydalar toplusunu şəbəkənin administratoruna analiz etməyə imkan verir.

RU-CERT
Korporativ şəbəkələrdə informasiya təhlükəsizliyinin pozulmalarının qeydiyyatını aparan təşkilat.

SAM – *Security Accounts Manager*
Korporativ şəbəkənin istifadəçilərinin qeydiyyat yazıları saxlanılan mühafizəli verilənlər bazası.

Seanslar
İstifadəçinin korporativ şəbəkəyə daxil olduğu andan çıxış anına qədər olan dövr.

Sendmail attack
SMTP portuna yönəlmiş hücumlar.

Server
1) Digər kompüterlərə şəbəkə vasitəsi ilə yardım göstərən və onları idarə edən güclü texniki parametrlərə malik olan kompüter 2) Digər (klient) proqramlara yardım edən və onların işini daim nəzarətdə saxlayan proqram vasitəsi.

Shadow Copy Restore
Windows əməliyyat sistemlərində faylların köhnə versiyalarını bərpa etmək üçün vasitə.

Shareware
Proqram təminatının yayılma modelidir. Bu halda proqramı almadan öncə onu sınaqdan keçirmək ("try before you buy") mümkündür.

Sxem – *Scheme*
Sxem – kataloqda yerləşdirilməsi ehtimal olunan bütün obyektlərin və atributların formal təyin olunmasıdır.

SID - *Security IDentifier*
Domenin mühafizəsi identifikatoru.

SID süzgəc
Etibar olunan meşənin əsas domenindən etibar edən meşənin əsas domeninə yoxlanılmış verilənlərin ötürülməsi zamanı baş verir.

Sistem jurnalları
İxtiyari serverin əməliyyat sisteminin daxilində baş verən bütün hadisələri və serverin işləməsində əngəl törədən sistem proqram təminatında sapmaların yaranma səbəbi olan hadisələr toplusunu qeydə alan bir sistem vasitəsi.

SMS – *Microsoft Systems Management Server*
Korporativ şəbəkələrdə proqram vasitələrinin quraşdırılması zamanı cədvəl üzrə işin təşkili, inventarlaşdırma, hesabatlılıq və şəbəkə üzərindən quraşdırma funksiyalarını yerinə yetirən proqram vasitəsi.

SMTP – *Simple Mail Transfer Protocol*
TCP/IP şəbəkələrində elektron poçtun ötürülməsi üçün nəzərdə tutulmuş şəbəkə protokolu

Smurf
ICMP Echo–cavablarını hücum olunan qovşağa külli miqdarda lazımsız informasiya şəklində generasiya edir.

SNA – *Systems Network Architecture*
Sistemin şəbəkə arxitekturası – IBM korporasiyası tərəfindən işlənib hazırlanmışdır. IBM proqramları ilə avadanlıq arasında olan məlumat mübadiləsi zamanı istifadə olunan strukturun, formatların, xüsusi elektron cədvəllərin, protokolların ümumi təsviridir.

Sniffer
Ötürülmə zamanı verilənlərin ələ keçirilməsində ən çox istifadə olunan metodlardan olan, şəbəkə vasitələrinin analizatoru və ya sniffer adlanan informasiya selinin yoxlama vasitələri.

SNMP – *Simple Network Management Protocol*
TCP/IP arxitekturası əsasında şəbəkələri idarə edən protokol.

SOAP – *Simple Object Access Protocol*
Paylanmış hesablama mühitində strukturlaşdırılmış məlumatların qarşılıqlı dəyişdirilməsinin protokolu. İlkin olaraq SOAP protokolu məsafədə olan prosedurların çağırılmasını (RPC) realizə etmək üçün nəzərdə tutulmuşdur. Məhz bu səbəbdən ona – obyektlərə girişin sadə protokolu adını vermişlər. İndi isə bu protokol, yalnız məsafədə olan prosedurların çağırılmasını deyil, həmçinin XML formatda olan ixtiyari məlumatların qarşılıqlı dəyişdirilməsi zamanı istifadə olunur.

Software Installation
Proqram təminatının işçi stansiyalara yüklənilməsi.

Spoofing
Bu tip hücumların ən çox yayılan variantı impersonasiya (qoşulmanın imitasiyasıdır, spoofing). İmpersonasiya zamanı bədəməl şəxsin qovşağı imitasiya etdiyi qovşağın üstünlüklərindən istifadə etmək üçün özünü digər qovşaq kimi qələmə verir.

Statgraphics proqramı
Statistik analiz və müxtəlif hesabatlar etmək üçün geniş imkanlı və qrafik interfeysli proqram təminatı.

SUS –
Software Update Sistem
Korporativ şəbəkənin serverlərində proqram təminatının yeniləşdirilmə xidməti.

SYN Flood (Neptune)
Bədəməl şəxs tərəfindən hücum edilən qovşağın emal edə biləcəyindən dəfələrlə çox miqdarda SYN seqmentlərinin göndərilməsindən ibarətdir.

SYN seqmenti – *Synchronize Sequence Numbers*
Ardıcıllıq nömrələrinin sinxronlaşdırılması.

Şəbəkə Administratoru
Kompüter şəbəkəsinin fasiləsiz və daim texniki saz vəziyyətdə işləməsinə cavabdeh olan şəxs.

Şəbəkənin idarəetmə elementləri
Şəbəkə üçün nəzərdə tutulmuş xüsusi təyinatlı proqram vasitələri başa düşülür. Məsələn: P sTools, Remote.exe (Support Tools).

Tam təhlükəsizlik rejimi – *Full Security*
Administratordan fərqli olan digər statuslu istifadəçilər "HKEY_LOCAL_MACHINE" reyestr açarını dəyişdirə bilməz və faylları öz profillərinə məxsus qovluqlardan başqa heç bir yerə yaza bilməzlər.

Tamlıq
İnformasiyanın saxlanması, ötürülməsi və emalı zamanı ilkin variantda və keyfiyyətdə qalmasının təminatı.

TCP/IP
İnternetdə informasiya mübadiləsinin əsasını təşkil edən şəbəkə protokolları.

Telnet
Başqa kompüterin məsafədən terminal kimi idarə olunması.

Telnet attack
Telnet protokolunda olan boşluqlardan istifadəyə yönələn hücum tipi.

Terminal Server
İstifadəçilərə ixtiyari məsələlərin həlli üçün hesablama resurslarını

təklif edən server.

Təhlükəsizlik parametrləri – Komponentinə təhlükəsizlik şablonu yükləməklə bir neçə kompüterin konfiqurasiyasını dəyişmək imkanı olan göstəricilər.

Təhlükəsizlik servisləri – Korporativ şəbəkədə yalnız təhlükəsizlik və mühafizə xidmətlərini təmin edən vasitə.

Təhlükəsizlik siyasəti – İnformasiyanın idarə olunmasını, təhlükəsizliyini və paylanmasını tənzimləyən normalar, qaydalar və praktiki nümunələr toplusu.

Təhlükəsizlik şablonları – *Security templates* – Təhlükəsizlik parametrlərini daxilində saxlayan fayllar.

Tətbiqi bölmələr – Adların konteksti təhlükəsizlik iştirakçılarından başqa ixtiyari tip obyektlərin iyerarxiyasını özündə saxlaya bilər.

Trialware – Proqram təminatının yayılma modelidir. Bu halda proqramdan istifadə müddəti məhduddur və göstərilən zaman bitdikdə proqram öz fəaliyyətini dayandırır. Trialware modeli proqramın istifadəçinin tələblərinə uyğun olmasını yoxlamağa imkanı verir.

Trusted namespace – *adların etibarlı fəzası* – Korporativ şəbəkənin meşələrarası etibar münasibətləri ilə bağlı olan adların etibarlı fəzası.

Trusted publishers – *proqram təminatının etibarlı istehsalçıları* – Əməliyyat sistemi tərəfindən tanınan proqram təminatı istehsalçılarılarının siyahısı.

TTL - *Time To Live* – Active Directory xidmətində dinamik yazılar üçün fəaliyyət müddəti.

UDDI – *Universal Description Discovery & Integration* – Digər təşkilatlar tərəfindən axtarışı və öz sistemlərinə inteqrasiya olunması üçün nəzərdə tutulan veb-servis şərhlərinin yerləşdirilməsi (WSDL) məqsədi ilə istifadə olunan alət.

UDP – *User Datagram Protocol* – İstifadəçi dataqramlarının protokolu. IP şəbəkələrində informasiya ötürmək üçün nəzərdə tutulmuş şəbəkə protokolu.

UDP flood – Külli miqdarda UDP-məlumatlar vasitəsi ilə reallaşan və kompüter şəbəkəsini dağıdılmasına yönələn çevik hücum növü.

URL - *Uniform Resource Locator*
Resursun yerini təyin edən vahid ünvan.

USMT – *User State Migration Tool*
İstifadəçilərin Miqrasiya Aləti vasitəsi korporativ şəbəkənin çox saylı istifadəçilərinin fayl və parametrlərinin miqrasiya prosesini sadələşdirir.

Veb-server
Adi veb brauzerlərdən istifadəçilərin HTTP-sorğularını qəbul edən və əvəzinə onlara HTTP–cavabları şəkillər, fayllar, media selləri, HTML səhifəsi, və s. bu kimi informasiyalar ilə birlikdə qaytaran güclü texniki imkanlara malik olan serverdir. veb server İnternetin özəyini təşkil edən vasitələrdən biridir.

Veb-servis
Bu xidmətin köməyi ilə ixtiyari proqramın funksiyaları İnternet vasitəsi ilə istifadə oluna bilər. Beləki PHP, ASP, JSP skriptlər, JavaBeans, COM-obyektləri və digər proqramlaşdırma dilləri başqa serverdə işləyən proqrama müraciət edib və alınan cavabı öz veb-saytında və ya proqramında istifadə edə bilər.

Verilənlər Trafiki
Vahid zaman ərzində müəyyən olunmuş nöqtədən keçən verilənlərin miqdarı ilə xarakterizə olunan şəbəkə parametri.

Verilənlərin miqrasiyası
Korporativ şəbəkəyə məxsus istifadəçinin verilənlərinin bir sistemdən digər sistemə keçirilməsi prosesi.

VxD – *Virtual Device drive*
MS Windows Server 2003 əməliyyat sisteminin virtual qurğularının yadda saxlanıldığı məkan.

Volume Shadow Copy
Verilmiş zaman kəsiyində şəbəkə kataloqlarının tərkibinin ehtiyat nüsxəsinin çıxarılmasını təşkil edən fayl xidməti.

Volume Shadow Copy Restore vasitəsi
Korporativ şəbəkənin administratorlarına xidməti dayandırmadan lazımi informasiyanın ehtiyat nüsxəsinin çıxarılması imkanını verir.

VRFY - *verify*
Kompüter şəbəkələrində informasiya mübadiləsi zamanı SMTP protokolunun daxili komandası olub, şəbəkə istifadəçisinin adını yoxlayır.

WAB – *Windows Address Book*
Şəxsi kontakt məlumatlarını yadda saxlamaq üçün MS

Windows əməliyyat sistemi tərəfindən təklif olunan poqram və xidmət.

WebDAV – *Web Based Distributed Authoring and Versioning*
Məsafədə olan məlumatların korporativ şəbəkə daxilində birgə istifadə olunması texnologiyası.

Windows Media Services
MS Windows Server 2003 əməliyyat sistemi tərəfindən dəstəklənən media sellərinin ötürülmə xidməti.

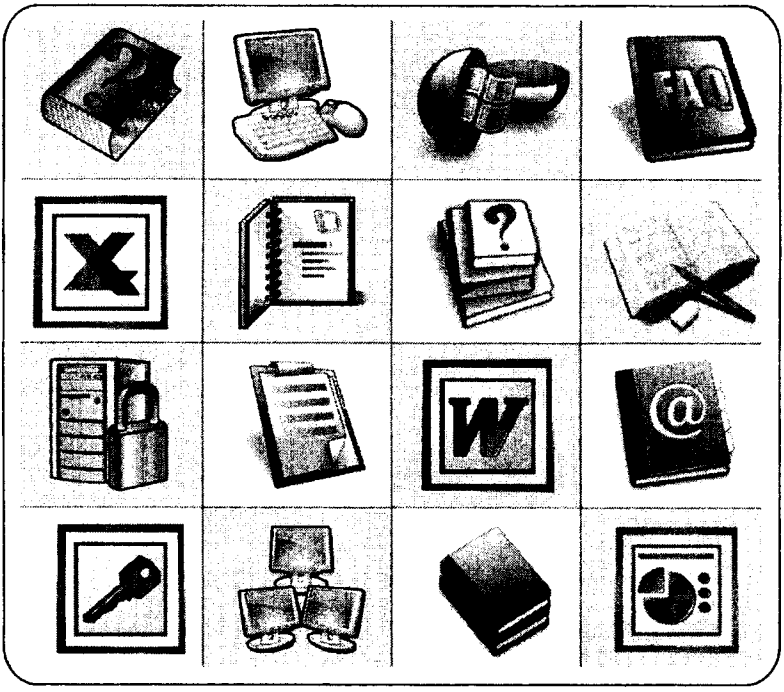
WinNuke / Out of Band ("növbəsiz") rejimi
Bu rejimdə 139-cu port (NetBIOS Session /SMB) TCP – qoşulması üçün URGENT bayraqlı verilənlər göndərir.

WMI – *Windows Management Instrumentation*
Windows əməliyyat sistemləri ailəsində idarəetmə alətləri. Komanda sətrinin sadə interfeysini təklif edir və mövcud komanda prosessoru (shell) ilə qarşılıqlı əlaqədə işləyir. Həmçinin ssenarilər vasitəsi ilə asanlıqla genişləndirilmək imkanına malikdir.

WSDL – *Web Services Description Language*
XML proqramlaşdırma dili əsasında yaradılan veb-servislərin şərhlərini yaratmaq üçün nəzərdə tutulan proqramlaşdırma dili.

Zəiflədilmiş təhlükəsizlik – *Relaxed Security*
Korporativ şəbəkənin adi istifadəçiləri üçün serverin parametrlərinin bəzilərini qismən dəyişdirmək imkanı olduğu hal.

Qeyd:
Əgər bir terminin izahı zamanı digər termin və ya abriviatura istifadə olunmuşdursa, onların izahı da əlifba sırasına uyğun olarq ayrıca verilmişdir.



İSTİFADƏ OLUNMUŞ

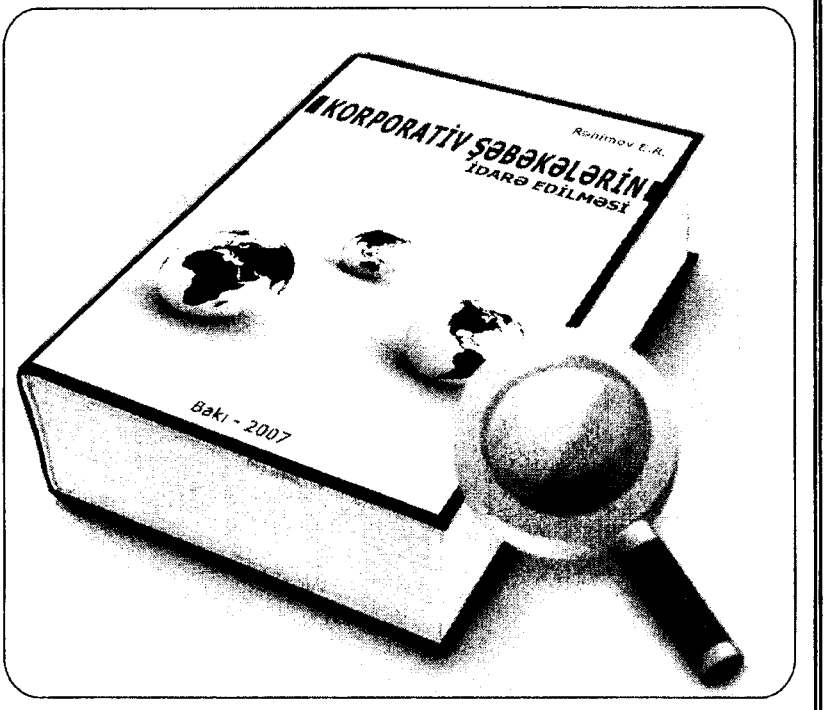
ƏDƏBİYYAT

İSTİFADƏ OLUNMUŞ ƏDƏBİYYAT

1. Алгулиев Р.М. Методы синтеза адаптивных систем обеспечения информационной безопасности корпоративных сетей.- М., Изд-во "ИСА РАН", 2001.
2. Алгулиев Р.М., Рагимов Э.Р. Нечеткая модель оценки информационной безопасности в корпоративных сетях // Автоматика и вычислительная техника. № 3, с. 66–74, Рига - 2005.
3. Алгулиев Р.М., Рагимов Э.Р. Об одном методе оценки информационной безопасности корпоративных сетей в стадии их проектирования // Информационные технологии. № 7, с. 35 – 39, Москва - 2005.
4. Борисов А.Н., Крумбег О.А., Федоров И.П. Принятие решение на основе нечетких моделей. Примеры использования .- Рига: "Зинатне", 1990.
5. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети. Анализ технологий и синтез решений. Спб: ДМК пресс, 2004.
6. Девянин П.Н., Михальский О.О., Правиков Д.И., Теоретические основы компьютерной безопасности. М.: Радио и связь, 2000.
7. Дезмонд М., Мидра М., Рампинг Б., Коррел Б. Windows 2000 Professional. Москва: Вильямс, 2001.
8. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. - ООО «ТИД ДС», 2001.
9. Завгородний В.И.. Комплексная защита информации в компьютерных системах. М: - Логос 2001.
10. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000.

11. Липаев В.В. Выбор и оценивание характеристик качества программных средств. М.: Синтег, 2001.
12. Попов А., Шикин Е. Администрирование Windows с помощью WMI и WMIC. Спб.: БХВ-Петербург, 2004.
13. Рагимов Э.Р. Классификация угроз по сервисам безопасности на основе статистических данных / Материалы VII Международной научно-практической конференции Информационная безопасность. Тагонрог: ТГРУ, 2005.
14. Рагимов Э.Р. Об одном подходе оценки риска при проектирование защищенных корпоративных сетей // Информационные технологии моделирования и управления. № 1(26), с. 94-98, Москва - 2006.
15. Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях. М.: Яхтсмен, 1993.
16. Трич Б. Microsoft Windows Server 2003. Службы терминала. Москва: Эком, 2006.
17. Уткин Л.В., Нетрадиционые методы оценки надежности информационных систем. – Спб.: Любович, 2000.
18. Уэнстром М. Организация защиты сетей Cisco. Москва: Вильямс, 2003.
19. Bertsekas D., Galleger R. Data Networks. London: Prentice-Hall Inc, 1992.
20. Cerven P. Crackproof Your Software – The Best Ways to Protect Your Software Against Crackers – San Francisco: NO STARCH PRESS, 2002.
21. Garfinkel S. Database Nation. Publisher: O'Reilly; ISBN: 0-596-00105-3, 2001.
22. JANET-CERT Report Statistics // http://www.ja.net.
23. ISO 2382-3:1987 // Information processing systems -- Vocabulary -- Part 3: Equipment technology.
24. ISO 2382-12:1988 // Information processing systems -- Vocabulary -- Part 12: Peripheral equipment.

25. ISO 9241-4:1998 // Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 4: Keyboard requirements.
26. ISO/IEC 2382-4:1999 // Information technology -- Vocabulary -- Part 4: Organization of data.
27. ISO/IEC 9995-1:2006 // Information technology -- Keyboard layouts for text and office systems -- Part 1: General principles governing keyboard layouts.
28. ISO 9241-400:2007 // Ergonomics of human--system interaction -- Part 400: Principles and requirements for physical input devices
29. Kevin S. Novell's Dictionary of Networking. Publisher: Novell Press; ISBN: 0-7645-4528-0, 1997.
30. Merabti M., Shi Q. and Oppliger R. Advanced security techniques for network protection // Computer Communications, vol. 23, 2000.
31. Pham H. Software reliability, Springer - Verlag, Singapore Ltd., 2000.
32. Pressman R.S. Software engineering. A practioner's approach. Singapore: McGraw-Hill, 1997.
33. Robichaux P. Secure Messaging with Microsoft Exchange Server 2000. Publisher: Microsoft Press; ISBN: 0735618763, 2003.
34. Ruley J.D. Networking Windows NT 4.0: Workstation and Server. Publisher: Wiley, John & Sons, Incorporated; ISBN: 0471175021, 1996.
35. Shinder T., Shinder D., Grasdal M. Configuring ISA server 2000. Publisher: Syngress Media Inc; ISBN: 1928994296, 2001.
36. Stallings W. Operating Systems: Internals and Design Principles. Publisher: Prentice Hall; ISBN: 0-13-031999-6, 2000.


KORPORATİV ŞƏBƏKƏLƏRİN
İDARƏ EDİLMƏSİ
Rəhimov E.R.
Bakı - 2007

İNDEKS

İNDEKS

Azərbaycan Milli Elmlər Akademiyası

İNFORMASİYA TEXNOLOGİYALARI İNSTİTUTU

«İnformasiya Texnologiyaları» nəşriyyatı

AZ 1141, Bakı şəh., F.Ağayev, 9

Tel.: (+99412) 510 42 74 Faks: (+99412) 439 61 21

secretary@iit.ab.az, www.science.az

Çapa imzalanmışdır 18.08.2007. Çap vərəqi 60x84 1/16,

Sifariş №9. Tiraj: 500