AUTOMATYKA • 2009 • Tom 13 • Zeszyt 3

Zdzisława Rowińska*

Wdrażanie sytemu Microsoft Windows 2003 Server i Active Directory w dużej firmie o zasięgu międzynarodowym

1. Wprowadzenie

Artykuł przedstawia proces wdrażania i konfiguracji (AD – *Active Directory*) w systemie *Microsoft Windows 2003 Serwer* na przykładzie jednej z dużych firm konsultingowych. Opisane zostały mechanizmy konfiguracji obiektów w konsolach administracyjnych usługi *AD* oraz procesy tworzenia kont użytkowników, komputerów i grup przy jednoczesnym zachowaniu standaryzacji nazw, która została wprowadzona w regionie CEE firmy. Omawiana firma jest największą na świecie organizacją świadczącą profesjonalne usługi doradcze. Zatrudnia ona 130 000 pracowników w 148 krajach, w Polsce posiada placówki w Warszawie, Krakowie, Gdańsku, Wrocławiu, Poznaniu i Katowicach. Zespół ten liczy ponad 880 specjalistów.

Obecna struktura sieciowa firmy w Europie oparta jest na kilku sieciowych systemach operacyjnych, zaistniała zatem potrzeba wprowadzenia jednolitej, hierarchicznie ułożonej struktury sieciowej jaką zapewnia system *Microsoft Windows 2003 Server* i *AD*.

Omawiana firma posiada kilkadziesiąt placówek na terenie regionu CEE. Każda z nich dysponuje własną, niezależną strukturą. Powoduje to odseparowanie i izolację logiczną sieci. Biura używają różnych systemów sieciowych jak *Novell 4.x, Novell 5.x.*, Windows NT, Windows 2000 i Windows 2003, dlatego oprócz fizycznego powiązania, na poziomie sieciowym nie są stworzone żadne logiczne struktury wewnętrzne pomiędzy regionami.

Najważniejsze problemy występujące w istniejącej strukturze regionów wchodzących w skład firmy to:

- brak centralnego systemu zarządzania siecią, także jako problem implementacji firmowych zasad bezpieczeństwa;
- brak skutecznej metody przypisania i zarządzania bezpieczeństwem wszystkich użytkowników, stacji roboczych, serwerów i obiektów aplikacji;

* Katedra Informatyki Stosowanej, Politechnika Łódzka

- brak możliwości globalnych zmian konfiguracji serwerów, stacji roboczych i aplikacji;
- dołączanie nowych zasobów nie może być dokonane z centralnego punku zarządzania tylko poprzez operacje lokalne;
- zróżnicowane schematy nazw utrudniają wykonywanie obowiązków pracownikom podróżującym między biurami;
- wprowadzenie nowych terytoriów do CEE jest operacją kosztowną pod względem konfiguracji i utrzymania sieci;
- uwierzytelnianie – brak centralnego punktu logowania;
- zasoby sieciowe są przypisane jedynie do regionów w których się znajdują, stwarza to problem wymiany danych i zarządzania projektami pomiędzy placówkami;
- brak możliwości kontrolowania dostępu do usług sieciowych na terytoriach CEE z centralnego punku zarządzania;
- konieczność duplikowania kont i uprawnień dla użytkowników podróżujących między biurami;
- dystrybucja i zarządzanie oprogramowaniem – brak standardowej metody dystrybucji oprogramowania i poprawności licencyjnej;
- brak centralnej metody dystrybucji poprawek systemowych i bezpieczeństwa, baz antywirusowych, *upgrade* aplikacji;
- brak możliwość kontrolowania instalacji nielegalnego oprogramowania na stacjach roboczych z ogólnodostępnego Internetu;
- nadmiar pracy administracyjnej IT, konieczność ponownej konfiguracji dla użytkowników przemieszczających się między regionami, utrudniona zdalna kontrola;
- system operacyjny stacji roboczych – problem z integracją z *Novell Netware*, konieczność utrzymania oddzielnych kont do stacji roboczych;
- w przypadku awarii systemu sieciowego w danym regionie, aby przenieść wszystkich użytkowników do nowej lokacji istnieje konieczność stworzenia całej struktury od nowa;
- brak kontroli bieżących sesji;
- ograniczony dostęp do aplikacji używanych w innym regionie CEE, ograniczony dostęp do danych poza biurem;
- konieczność poznania przez użytkownika dokładnej lokalizacji poszukiwanych zasobów.

Powyższe problemy można rozwiązać poprzez wprowadzenie *AD* wraz z systemem Microsoft Windows 2003 Server.

Stworzenie ujednoliconej infrastruktury sieciowej w firmie umożliwi dostęp do zasobów poszczególnych regionów poprzez zcentralizowane zarządzanie. Zastąpienie obecnego systemu sieciowego produktem *Windows 2003 Server* umożliwi maksymalne wykorzystanie możliwości systemów operacyjnych na stacjach roboczych, natomiast wdrożenie *Microsoft Systems Management Server* pozwoli zarówno dystrybuować oprogramowanie,

zarządzać sprzętem używanym przez użytkowników, jak i kontrolować oprogramowanie zainstalowane na stacjach roboczych we wszystkich oddziałach firmy.

Wprowadzenie nowego regionu stanie się łatwiejsze na platformie Windows wraz z gotowymi ustawieniami systemów finansowych zarządzania dokumentami.

Najważniejszym jednak aspektem biznesowym jest wzrost efektywności pracowników poprzez możliwość współdzielenia doświadczeń, dokumentów i wiedzy między poszczególnymi regionami.

2. Struktura logiczna Active Directory

2.1. Struktura lasu i poziomy funkcjonalności domeny

Domena jest główną jednostką administracyjną usługi katalogowej Windows Server 2003 i istnieje ścisła zależność pomiędzy jej istnieniem a *AD*.

W usłudze *AD* przedsiębiorstwo może posiadać wiele domen. Tworzą one wtedy strukturę nazywaną drzewami przy jednoczesnym zachowaniu struktury hierarchicznej nazw DNS. W sytuacji, gdy domeny *AD* nie tworzą jednej domeny, oznacza to, że tworzą tzw. las – zawiera on wszystkie drzewa usługi. Domena nie może istnieć samodzielnie, musi znajdować się w jakimś drzewie, a tym samym lesie.

Poziomy funkcjonalności domeny określają, jakie funkcje systemowe i sieciowe mogą być wykorzystane. Występują cztery poziomy funkcjonalności: mieszany Windows 2000, macierzysty Windows 2000, tymczasowy Windows Server 2003 i Windows Server 2003. Środowisko, w jakim system na być zainstalowany decyduje o funkcjonalności, jako domyślny przypisywany jest poziom mieszany.

Opcja, w której najbardziej wykorzystane są możliwości systemu, jest Windows Server 2003. Dostępne są wtedy wszystkie funkcje na poziomie domeny lub lasu. Pozostałe spotykają się z ograniczeniami wynikającymi z różnic technologicznych pomiędzy wersjami systemu operacyjnego. Przykładem może być możliwość tworzenia grup uniwersalnych, która jest całkowicie wyłączone w systemie mieszanym 2000, a dozwolona w macierzystym 2000 i 2003 zarówno dla grup zabezpieczeń, jak i grup dystrybucyjnych. Podobna sytuacja występuje przy konwersji grup z dystrybucyjnej na zabezpieczeń, także w opcji mieszanej 2000 jest ona niewykonalna.

Active Directory jest obiektową bazą danych, w której informacje ułożone są w sposób hierarchiczny. Obiektami są tutaj użytkownicy, aplikacje czy też zasoby sieciowe. Podstawową jednostką jest liść, znajdujący się w jednostce organizacyjnej, czyli *Organizational Unit*. Obiekty te organizowane są w domeny. Te natomiast zorganizowane hierarchicznie tworzą struktury drzewa. Drzewo powinno posiadać przynajmniej jedną domenę zwaną korzeniem drzewa. Pozostałe domeny umieszczane są poniżej w strukturze katalogowej.

Domeny w usłudze katalogowej korzystają z tej samej przestrzeni nazw DNS. Posiadają ten sam korzeń, a kolejne nazwy powstają poprzez dodanie nazwy do domeny wyższego poziomu.

W omawianej firmie przyjęto następujące oznaczenia: (Cee – *Central and Eastern Europe*); (Ema – *Europe*) and middle *Asia*; (AD – *Active Directory*). Pełna nazwa: Cee.ema.ad.pwcinternal.com.

Active Directory oparto na pojedynczej strukturze domeny. Ponieważ nie jest wymagana niezależność bądź też izolacja zasobów w poszczególnych regionach CEE najlepszym rozwiązaniem jest pojedynczy las, pojedynczej domeny. Wszystkie stacje robocze wyposażono w system operacyjny *Microsoft Windows XP* z dodatkiem SP2. Pozwala to osiągnąć poziom funkcjonalności Windows Serwer 2003, sprzyja łatwości w zarządzaniu i rozwiązywaniu problemów, a także utrzymaniu modelu struktury katalogowej.

2.2. Nazewnictwo Active Directory

W tworzeniu struktury katalogowej *AD* istotnym zagadnieniem jest opracowanie unikalnych schematów nazewnictwa poszczególnych obiektów. Użytkownicy, grupy, jednostki, zasoby sieciowe powinny posiadać nazwę, która będzie określała ich przynależność do danego regionu, działu czy też funkcji pełnionej w firmie bądź systemie.

Wszystkie skróty odnoszą się do anglojęzycznych nazw, odpowiednio do funkcji serwera w systemie. Użyty został następujący wzorzec:

NazwaKraju(2)-NazwaMiasta(3)TypSerwera(3)Numer(3)

NazwaKraju – składa się z pierwszych dwóch znaków identyfikujących dane państwo. Została oparta na standardzie ISO 3166-1.

NazwaMiasta – identyfikator oparty o IATA *CityCodes* – międzynarodowy standard oznaczania lotnisk.

TypSerwera – oznaczenie serwera udostępniającego daną usługę.

Przykładowe oznaczenie serwera (MOM – *Micorsof Oparation Manager*), znajdującego się w Warszawie, oznaczonego numerem 001: *PL-WAWMOM001.*

Oznaczenia stacji roboczych tworzone są poprzez sumę identyfikatora państwa i określonego numeru porządkowego np.: *PL-006430, CZ-100422.*

2.3. Obiekty Active Directory

Przy tworzeniu obiektów *AD* obowiązują te same zasady nazewnictwa. Lokacje (*sites*) opierają na istniejącej strukturze sieciowej firmy. Użyto formatu składającego się z oznaczenia państwa i pełnej nazwy miasta. Zostały one stworzone jedynie dla miast posiadających przynajmniej jeden kontroler domeny.

NazwaKraju(2)-NazwaMiasta

Przykładowe lokacje: *PL-Warsaw*, *RU-Moscow*

Na istniejącej topologii sieci zostało oparte także nazewnictwo łącza między lokacjami (*sites-links*). Opiera się ono na schemacie:

[NazwaKraju(2)-NazwaMiasta]- -[NazwaKraju(2)-NazwaMiasta]

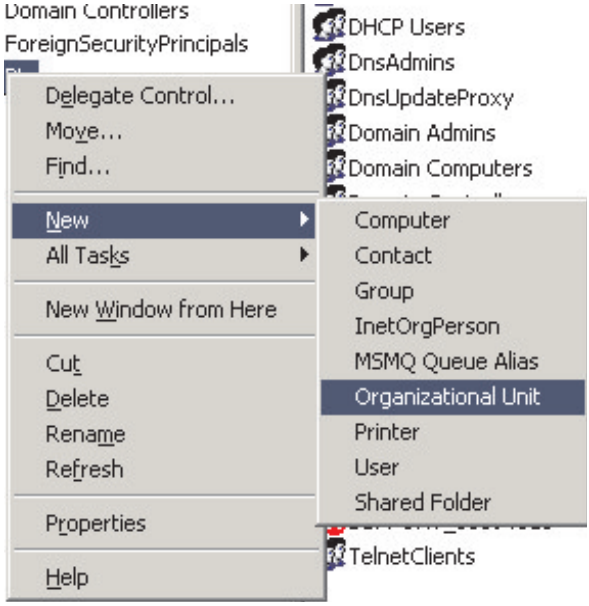
np.: *[PL-Warsaw]- - [CZ-Prague]* oznacza łącze pomiędzy Warszawą a Pragą.

3. Jednostki organizacyjne

3.1. Podział terytorialny i działowy

Usługa *AD* została stworzona, aby przechowywać miliony obiektów takich jak: użytkownicy i grupy, komputery, foldery, drukarki, zasoby sieciowe czy też zasady grup (GPO – *Group Policy Object*). Aby zarządzanie tak wielką ilością danych stało się prostsze opracowana została struktura, która organizuje je w odpowiednie grupy (OU – *Organizational Unit*).

Organizational Unit jest kontenerem umożliwiającym grupowanie obiektów w *AD* w zależności od ich przynależności administracyjnej lub konfiguracyjnej. OU tworzymy w konsoli administracyjnej *Active Directory Users and Computers*, wybierając opcję *Organizational Unit* (rys. 1).



Rys. 1. Tworzenie jednostki organizacyjnej

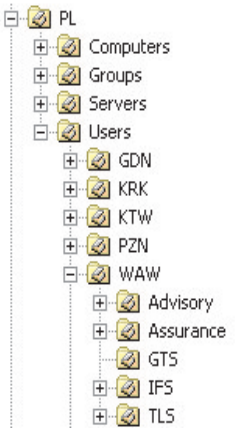
Najczęstszym sposobem organizacji danych w *AD* jest odwzorowanie struktury administracyjnej firmy w strukturę katalogową. W takim układzie działy odpowiadają poszczególnym jednostkom administracyjnym, a konta komputerów, użytkowników i grup znajdują się w odpowiadającym im kontenerach.

W omawianej firmie poszczególne regiony CEE zostały umieszczone w strukturze *AD* jako kontenery zawierające grupy, użytkowników i komputery należące do danego kraju. Jednostka OU została stworzona jedynie dla regionów posiadających kontroler domeny.

Także struktura działowa firmy została odpowiednio oznakowana (rys. 2) i odwzorowana w strukturze katalogowej (rys. 3).

Dział	Oznaczenie
Assurance Services	Assurance
Consumer & Industrial Products & Services	CIPS
Financial Services	FS
Technology InfoComm & Entertainment	TICE
Advisory Services	Advisory
Performance Improvement	PI
Transactions	TS
Tax and Legal Services	TLS
Human Resource Services	HRS
Internal Firm Services	IFS
GTS	GTS
Human Capital	HC
Marketing	M&C

Rys. 2. Odwzorowanie nazw działów na jednostki OU



Rys. 3. Układ jednostek organizacyjnych

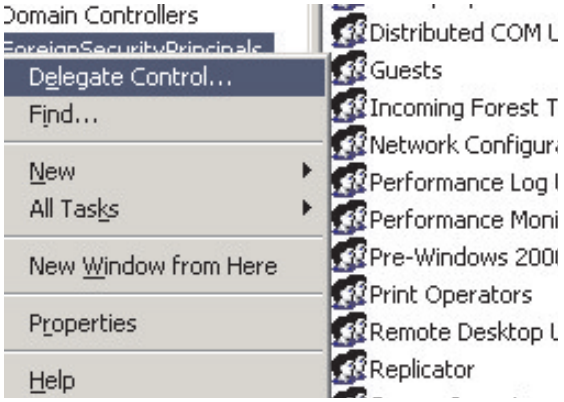
3.2. Specjalne jednostki organizacyjne

Istnieją pewne wbudowane jednostki organizacyjne, do których należą takie kontenery jak: *Builtin* zawierający konta wbudowane systemu m.in. *Account Operators*, *Backup Operators* czy też *Administrators*. Domyślnie znajdują się tu także jednostki *Domain Control-*

lers, mieszcząca kontrolery domeny, *Computers* i *Users* zawierająca odpowiednio użytkowników i komputery. Dodatkowo tworzone są specjalne jednostki organizacyjne, których celem jest dokładniejsze i bardziej przejrzyste zarządzanie zasobami *AD*.

Przykładem takiej jednostki może być kontener *Transfer.* Jest on stworzony specjalnie, aby umożliwić przenoszenie obiektów *AD*, użytkowników i komputery pomiędzy poszczególnymi jednostkami terytorialnymi. Administratorzy poszczególnych terytoriów posiadają dostęp tylko do jednostek swojego regionu, aby zapewnić możliwość transferu stworzono jednostkę *Transfer*, do której dostęp mają wszyscy administratorzy. Kolejnym przykładem jednostki specjalnej jest stworzenie jednostki zawierającej obiekty, użytkowników i grupy, posiadające wyższe uprawnienia administracyjne w *AD*. Jednostka *ServiceAdm* zawiera grupy administracyjne, konta administracyjne i konta poszczególnych usług.

Kontenery *AD* posiadają także inne funkcje administracyjne. Poprzez OU może być delegowany dostęp do poszczególnych zasobów, co w przypadku rozległej sieci zmniejsza nakład pracy administracyjnej poprzez rozłożenie obowiązków na poszczególnych administratorów. Delegować można dostęp do każdej jednostki w *AD*. Wykonuje się to poprzez wybranie z właściwości kontenera opcji *Delegate* (rys. 4). Przykładem takiego zarządzania może być nadanie odpowiedniemu konsultantowi uprawnienia pozwalającego na zmianę hasła użytkownika w danej jednostce.



Rys. 4. Delegowanie kontroli

4. Użytkownicy i grupy

Użytkownicy i grupy w *AD* zorganizowani są w poszczególne kontenery odpowiadające ich przynależności do funkcji systemu bądź też działów firmy. Podczas logowania następuje uwierzytelnienie na podstawie nazwy użytkownika, hasła i unikalnego identyfikatora SID. System na postawie tych danych tworzy tzw. żeton, który od tego momentu reprezentuje użytkownika w systemie. Na podstawie żetonu sprawdzana jest przynależność do gru-

py i odpowiedni dostęp do zasobów na podstawie (ACL – *Access Control List*). Użytkownicy tworzeni są w konsoli administracyjnej *Active Direcotry Users and Computers*.

Po określeniu tzw. loginu danego użytkownika i podaniu jego danych osobowych, określane są podstawowe informacje dotyczące konta. W firmie konta użytkowników oparto na unikalnym identyfikatorze (GUID – *Globally Unique Identifier*), który identyfikuje obiekty w systemie. Loginy składają się z kombinacji liter imienia i nazwiska użytkownika, zakończone numerem seryjnym, w przypadku identycznych danych osobowych, numer ten decyduje o unikatowości loginu.

Grupy można określić jako kontenery zawierające obiekty użytkowników, a także inne grupy. Poprzez grupy nadawany jest dostęp do poszczególnych zasobów sieciowych czy też obiektów *AD*. Operowanie grupami podczas określania ACL, zgodnie z zaleceniami firmy Microsoft powinno operować na grupach zabezpieczeń tzw. *Security Groups*.

System Microsoft Windows 2003 Serwer został wyposażony w dwa rodzaje grup: dystrybucyjne i zabezpieczeń. Grupy dystrybucyjne używane są przede wszystkim do tworzenia grup korespondencyjnych, natomiast grupy zabezpieczeń mogą służyć do przypisywania określonych dostępów do zasobów, a także mogą pełnić funkcje grup dystrybucyjnych. W odróżnieniu od poprzednich wersji systemów serwerowych firmy Microsoft, w wersji 2003 Serwer możliwe jest dokonanie konwersji grup dystrybucyjnych na grupy zabezpieczeń.

W systemie Microsoft Windows 2003 Serwer istnieją wbudowane konta użytkowników i grup Znajdują się one w jednostkach organizacyjnych *Builtin* i *Users*

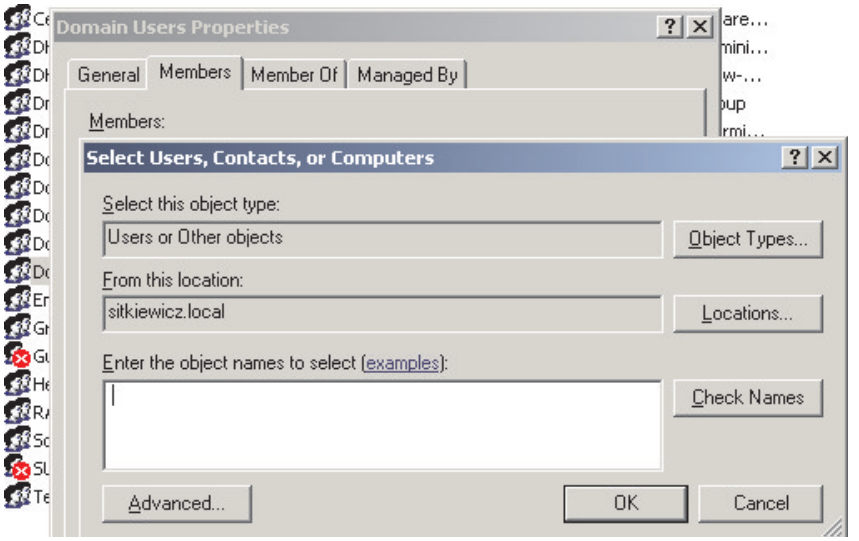
Grupy zawarte w jednostce *Builtin* zawierają grupy zabezpieczeń o zakresie domenowym lokalnym. Znajdują się tam m.in.

- *Account Operators* – operatorzy kont, członkowie tej grupy mogą zarządzać użytkownikami domeny i kontami grupy;
- *Administrators* – administratorzy, posiadają całkowite i nieograniczone uprawnienia do każdego obiektu systemu;
- *Print Operators* – operatorzy wydruku, członkowie administrują serwerami wydruku domeny;
- *Remote Desktop Users* – użytkownicy pulpitu zdalnego, członkowie tej grupy posiadają możliwość zdalnego logowania się do systemu.

W jednostce *Users* znajdują się takie obiekty jak:

- Konto administratora;
- *DNS Admins* – administratorzy usługi rozwiązywania nazw;
- *DHCP Administrators* – administratorzy usługi dynamicznego przydzielania adresów;
- *Domain Controllers* – kontrolery domeny;
- *Domain Users* – wszyscy użytkownicy domeny;
- *Domain Computers* – wszystkie komputery domeny.

Dodawanie użytkowników do grup odbywa się poprzez wybranie właściwości grupy i określenie na zakładce *Members* członków grupy (rys. 5).



Rys. 5. Określanie członkostwa grup

Nazwy grup powinny jednoznacznie określać funkcję, jaką grupa będzie sprawować w systemie. Schemat opracowany w firmie przedstawia się w następująco:

GL-KodKraju()KodMiasta(3)-OznaczenieGrupy()-Dział()-Opis()

Przykładowy opis grupy: GL-PLWAW-GRP-GTS -HelpDesk

Grupa globalna *HelpDesk* znajdująca się w Polsce, w Warszawie, zawierająca pracowników *help-desk*, działu *Global Technology Solutions*.

Kolejnym przykładem może być grupa: DL-PLWAW-APP-FIN-Sun

Grupa lokalna domenowa, znajdująca się w Polsce, w Warszawie, zawierająca aplikacje działu finansowego.

Aby umożliwić odpowiednie rozpoznawanie grup dodatkowo użyto następujących oznaczeń:

- *Application – APP* – używane jest, gdy głównym celem istnienia grupy jest zapewnienie dostępu do aplikacji;
- *Directory – Dir* – w przypadku, kiedy grupa ma decydować o dostępie do poszczególnych zasobów plików/katalogów;
- *Bussines Unit – GRP* – używane, kiedy grupa definiuje członkowstwo poszczególnych działów. Może, ale nie musi decydować o dostępie do zasobów sieciowych i systemowych uprawnieniach;
- *Printer – Prt* – używane w przypadku, kiedy członkowstwo decyduje o dostępie do drukarek;
- *Script – Scr* – członkowstwo decyduje o odpowiednich ustawieniach login skryptu;
- *Group Policy Filtering – GPO* – stosowana w przypadku, gdy grupa kontroluje filtrację zasad polityki grup.

5. Podsumowanie

Wprowadzając *Active Directory* wraz z systemem *Microsoft Windows 2003 Serwer* w firmie zrealizowano wszystkie założenia tego projektu. Stworzono centralny punkt zarządzania siecią firmową, umożliwiając odgórne określenie zasad bezpieczeństwa stacji roboczych i serwerów poprzez odpowiednie polityki GPO. Otrzymano możliwość dokonywania globalnych zmian w konfiguracji każdego komputera podłączonego do domeny CEE, ujednolicono także nazewnictwo obiektów systemu. Poprzez zastosowanie *Active Directory Microsoft Windows 2003 Serwer* zlikwidowano konieczność duplikacji kont systemowych i uzyskano maksymalne korzyści z wykorzystania systemu operacyjnego Microsoft Windows XP. Dodatkowo usprawniono dostęp do usług i zasobów sieciowych. Zintegrowanie *Active Directory* z systemem DNS umożliwiło szybkie przeszukiwanie nazw obiektów i prawidłowe odnajdywanie kontrolerów domeny, przy zachowaniu określonej hierarchii. Zastosowanie oprogramowania *Systems Management Serwer* współdziałającego z domeną Windows 2003 znacznie poprawiło system dystrybucji oprogramowania w postaci pakietów MSI. Najbardziej istotnym przejawem zmiany sieciowego systemu operacyjnego jest jednak zadowolenie pracowników z obecnego trybu pracy. Ułatwienie dostępu do zasobów sieciowych, jednolitość haseł, uproszczone procedury zdalnego dostępu do sieci firmowej czy prostota obsługi stanowią aspekty, które w zauważalny sposób wpłyną na usprawnienie pracy, a tym samym zwiększenie zysków przedsiębiorstwa.

Literatura

[1] Dan Holme, Orin T., *Zarządzanie i obsługa środowiska Microsoft Windows 2003 Serwer*. APN Promise Sp. z o.o. Warszawa 2004.

[2] Macikn J.C., McLean J., *Wdrażanie, zarządzanie i obsługa infrastruktury sieciowej Microsot Windows 2003 Serwer*. APN Promise Sp. z o.o. Warszawa 2004.

[3] *Materiały kursowe. Wdrażanie, zarządzanie i obsługa infrastruktury sieciowej Microsot Windows 2003 Serwer: usługi sieciowe*. Microsotf Corporation, 2005.

[4] *Materiały kursowe: Planowanie, zarządzanie i obsługa struktury Active Directory w systemie Microsoft Windows 2003 Serwer*. Microsotf Corporation, 2005.

[5] Richards J., Allen R., Lowe-Norris A., *TechTasks Code Center, Active Directory*. O'Reilly Media-Publication, 2006.