Ćwiczenie 2 Podstawowe zadania administracyjne

Cel ćwiczenia:

Zapoznanie się z podstawowymi zadaniami administracyjnymi systemu Windows 2000: zarządzanie kontami użytkowników i grup, ochrona plików i folderów.

Przed przystąpieniem do ćwiczenia uczeń powinien:

- umieć poruszać się po systemie Windows,
- umieć zarządzać plikami i folderami w systemie Windows,
- umieć zarządzać dyskami pod Windows 2000,
- umieć korzystać z narzędzi do rozwiązywania problemów w Windows 2000.

Po wykonaniu ćwiczenia uczeń będzie umiał:

- zakładać konta użytkownikom,
- ustawiać zaawansowane opcje kont,
- tworzyć i zarządzać kontami grup,
- korzystać z zasad konta,
- definiować prawa użytkowników i opcje zabezpieczeń,
- korzystać z lokalnych zasad grup,
- ustawiać uprawnienia do plików i folderów,
- kontrolować przydziały dyskowe,
- korzystać z kompresji i szyfrowania plików i folderów.

Uwagi o realizacji ćwiczenia:

Ćwiczenie podzielone jest na rozdziały. Rozdział zbudowany jest z opisu teoretycznego omawiającego wybrane zagadnienie i zadania do wykonania. Zadania umieszczone są w ramkach. Po wykonaniu zadania uczeń zobowiązany jest do przeprowadzenia samooceny, korzystając z punktacji 1-5. Nauczyciel może skorygować ocenę ucznia. Na końcu ćwiczenia znajduje się spis zadań.

W czasie tego ćwiczenia uczniowie pracują na oddzielnych komputerach wyposażonych w dwie karty sieciowe firmy 3Com: Fast EtherLink PCI 3C905C-TX i EtherLink ISA 3C509B. Karta 3C905C-TX powinna być podłączona do sieci lokalnej CKP.

Przed przystąpieniem do ćwiczenia uczeń powinien odświeżyć swój komputer z obrazu Windows 2000 Pro PL.

W czasie ćwiczenia uczeń ma do dyspozycji:

- płytę z obrazem Windows 2000 Pro PL.

2.1 Zarządzanie użytkownikami i grupami

2.1.a Wstęp

Jeżeli stacja Windows 2000 Professional nie pracuje w domenie NT lub 2000, wówczas dostęp do lokalnego komputera można ograniczyć przez wykorzystanie kont lokalnych użytkowników.

Podczas instalacji, tworzone jest konto ***Administrator***. Z tego konta użytkownik ma pełen dostęp do konfiguracji systemu i do wszystkich zasobów. Automatycznie tworzone jest także konto ***Gość***. Po instalacji konto to jest jednak zablokowane.

Konto użytkownika jest unikalnym zestawem danych uwierzytelniających użytkownika. Na konto składa się:

- Nazwa użytkownika - do (20 znaków) bez „<>[]:;|=,+*?<>
- Imię i Nazwisko
- Opis
- Hasło - do 128 znaków (uwaga: rozróżniana jest wielkość liter)

Jedynie osoba posiadająca konto może zalogować się do systemu. Administrator udostępnia system nadając użytkownikom prawa oraz uprawnienia. Wszystkie dane uwierzytelniające użytkownika kojarzone są z identyfikatorem zabezpieczeń (SID, Security Identifier) i podczas nadawania praw i uprawnień system korzysta właśnie z SID. Dzięki temu zmiana nazwy użytkownika nie zmienia jego praw i uprawnień w systemie. Natomiast usunięcie użytkownika z systemu i ponowne założenie konta o tej samej nazwie, spowoduje zmianę numeru SID, a zatem prawa i uprawnienia nie zostaną zachowane.

Aby uprościć administrację wieloma użytkownikami wprowadzono ***grupy***, których zadaniem jest połączenie wielu użytkowników w jeden obiekt, którym administrator może znacznie wygodniej zarządzać.

W czasie instalacji tworzonych jest kilka standardowych grup:

- ***Administratorzy*** **-** członkowie tej grupy mogą wykonać wszystkie zadania.
- ***Goście*** - grupa ta umożliwia nadanie ograniczonych uprawnień użytkownikom jednorazowym korzystającym z wbudowanego konta ***Gość***. Członkowie grupy ***Goście*** mogą także zamknąć komputer.
- ***Użytkownicy*** **-** normalni użytkownicy z ograniczeniami. W znacznej części systemu posiadają oni tylko uprawnienia odczytu. Nie mogą odczytywać danych należących do innych użytkowników, instalować aplikacji wymagających modyfikacji katalogów systemowych, ani wykonywać zadań administracyjnych.
- ***Użytkownicy zaawansowani*** - posiadają uprawnienia zapisu/odczytu w innych częściach systemu. Użytkownicy ci mogą instalować aplikacje i wykonywać zadania administracyjne.
- ***Operatorzy kopii zapasowej*** **-** członkowie tej grupy mogą utworzyć kopie zapasowe i odtworzyć pliki na komputerze, niezależne od ewentualnych uprawnień chroniących te pliki. Mogą także zalogować się na komputerze i zamknąć go, ale nie mogą zmieniać ustawień zabezpieczających.

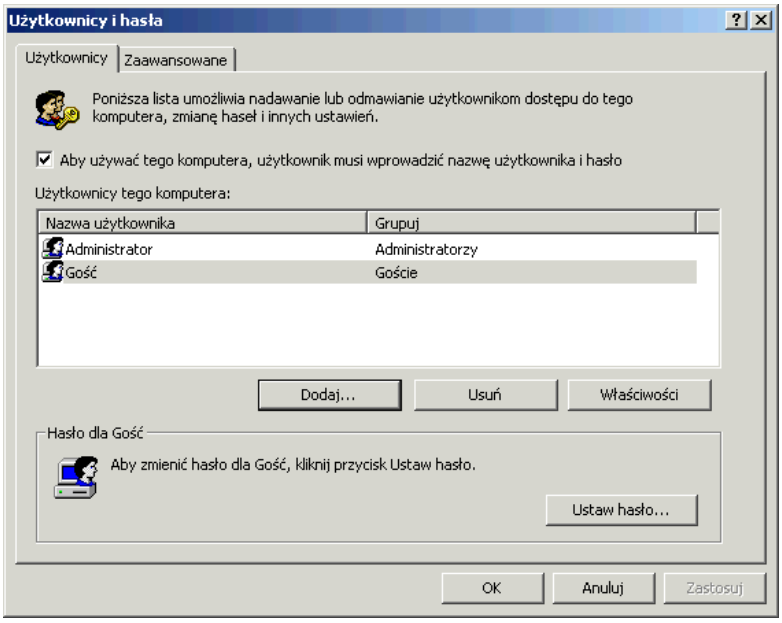
2.1.b Tworzenie konta lokalnego

W ***Panelu sterowania*** znajduje się ikona ***Użytkownicy i hasła***. Aby zabezpieczyć dostęp do lokalnego komputera, należy załączyć opcję ***Aby używać tego komputera, użytkownik musi wprowadzić nazwę użytkownika i hasło.***

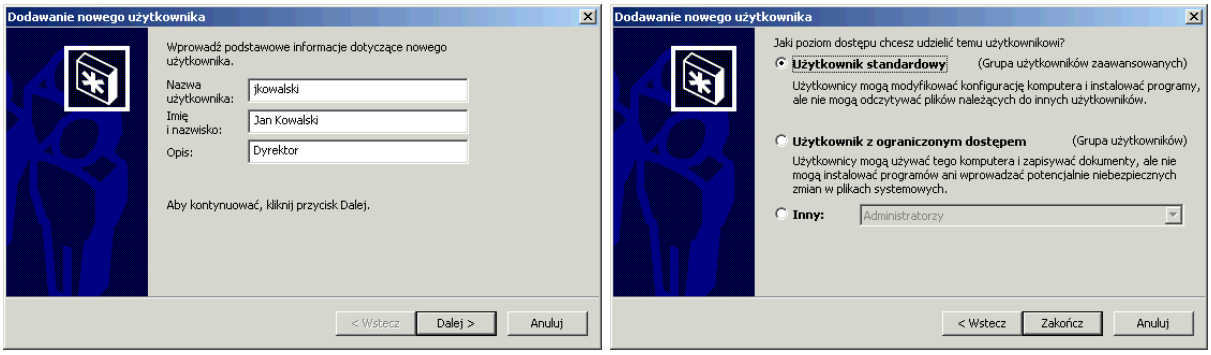
Aby dodać nowe konto dla użytkownika:

1. Należy kliknąć ***Dodaj*** i podać unikalną nazwę, imię i nazwisko i opcjonalnie opis. W nazwie konta można podać duże i małe litery, jednak nie będą one rozróżniane przez system. Warto też przyjąć konwencję nazewniczą dla nazwy konta np. pierwsza litera imienia i całe nazwisko.
2. Po wybraniu ***Dalej*** potwierdzić dwukrotnie hasło. Każde konto użytkownika powinno być chronione hasłem. Należy unikać haseł bardzo prostych jak: kombinacje imienia i nazwiska, imię ukochanej czy psa, numer telefonu zapisany od końca. Powinno się stosować długie hasła (do 128 znaków, zalecane min. 8) zawierające zarówno małe jak i duże litery, cyfry a także znaki specjalne jak. np. #$ *() i inne.
3. W ostatnim kroku należy określić przynależność do grupy.

Aby zmodyfikować właściwości konta korzysta się z przycisku ***Właściwości***. W celu zmiany hasła z przycisku ***Ustaw hasło***.



Rys. 2.1 Okno Użytkownicy i hasła



Rys. 2.2 Okna kreatora dodawania użytkownika

Zadanie 2.1.a – Zakładanie kont użytkowników

1. Utwórz konta dla użytkowników:

Imię i nazwisko	Nazwa użytkownika	Hasło	Grupa
Jan Kowalski	***jkowalski***	***jk309***	Użytkownik
Jan Kowalski	***jkowalski2***	***jk2309***	Użytkownik
Tadeusz Kargul	***tkargul***	***tk309***	Użytkownik zaawansowany
Aleksandra Nowak	***anowak***	***mn2000***	Użytkownik zaawansowany
Anna Pawlak	***apawlak***	***ap2000***	Użytkownik zaawansowany

2. Zmień przynależność do grup i hasła

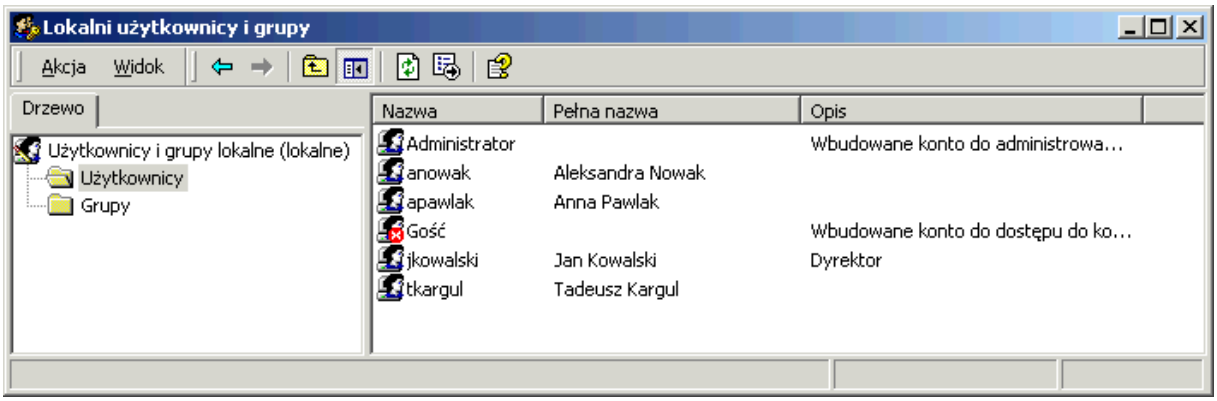
Imię i nazwisko	Nazwa użytkownika	Hasło	Grupa
Jan Kowalski	***jkowalski***	bez zmian	Użytkownik zaawansowany
Jan Kowalski	***jkowalski2***	bez zmian	Użytkownik zaawansowany
Tadeusz Kargul	***tkargul***	bez mian	Użytkownik
Aleksandra Nowak	***anowak***	***mn309***	Użytkownik
Anna Pawlak	***apawlak***	***ap309***	Użytkownik

3. Usuń konto ***jkowalski***.
4. Zmień nazwę konta ***jkowalski2*** na ***jkowalski***.

2.1.c Ustawienia zaawansowane kont

Na zakładce ***Zaawansowane*** w oknie ***Użytkownicy i hasła,*** po wybraniu przycisku ***Zawansowane,*** można zmieniać zaawansowane ustawienia kont. Wystarczy z listy kliknąć dwukrotnie wybranego użytkownika.

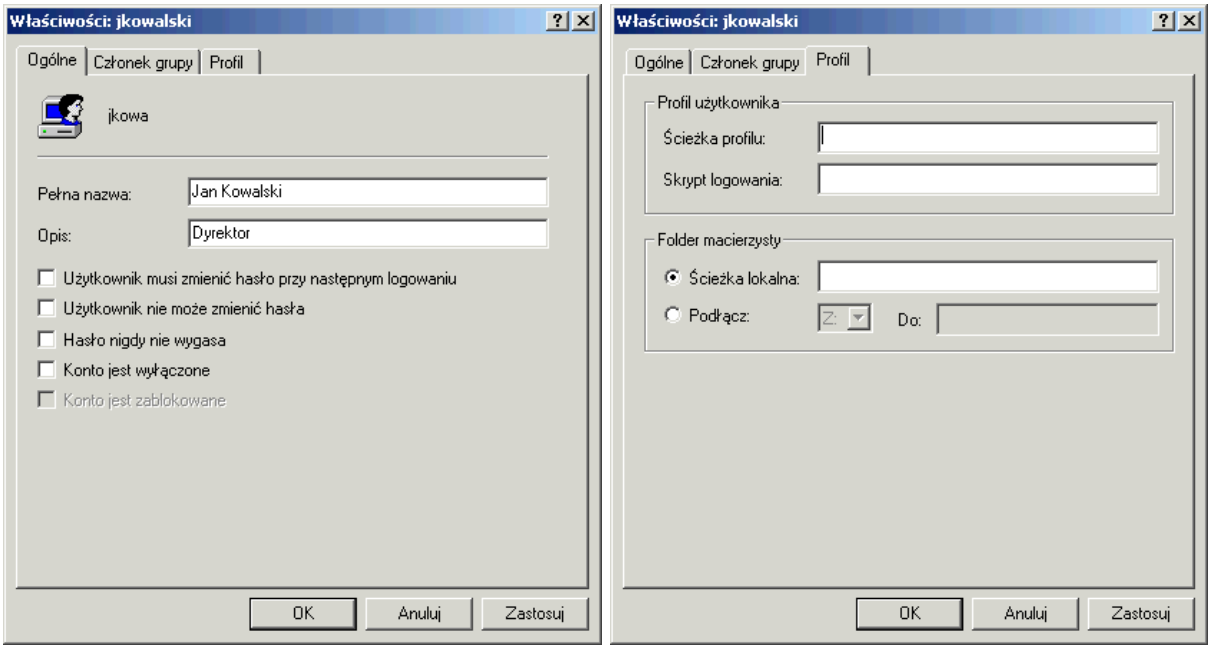
Jeżeli przy nazwie użytkownika widnieje biały x na czerwonym polu, oznacza to, iż konto jest zablokowane.



Rys. 2.3 Zarządzanie użytkownikami i grupami

W ustawieniach zaawansowanych znajdziemy zakładkę ***Ogólne***, a na niej możliwość załączenia jednej z poniższych opcji:

- ***Użytkownik musi zmienić hasło przy pierwszym zalogowaniu.*** Konto powinno chronić hasło wymyślone przez użytkownika danego konta. Dzięki tej opcji administrator może wymusić, aby użytkownik przy pierwszym zalogowaniu sam podał hasło dla konta.
- ***Użytkownik nie może zmienić hasła.*** Czasami administrator zakłada konto publiczne, z którego będzie korzystać kilka osób. Wówczas należy opcję tą załączyć, użytkownicy nie będą mogli zmieniać hasła.
- ***Hasło nigdy nie wygasa.*** Administrator w zasadach kont może wymusić na użytkownikach, aby ich hasła wygasały po pewnym czasie. Zwiększa to bezpieczeństwo systemu. W przypadku wybranych kont (np. publicznych – kilka osób korzysta z jednego konta) można wyłączyć wygasanie haseł.
- ***Konto jest wyłączone***. Jeżeli administrator chce czasowo zablokować konto, to powinien korzystać z tej opcji. W przypadku usunięcia i ponownego założenia konta o tej samej nazwie, użytkownik traci dostęp do zasobów.



Rys. 2.4 Okno właściwości zaawansowanych konta użytkownika

2.1.d Zmiana członkostwa w grupach

Na zakładce ***Członek grupy*** w oknie zaawansowanych właściwości konta użytkownika, można zmienić przynależność do grup. Użytkownik może należeć do kilku grup.

2.1.e Profile użytkownika

System Windows 2000 pozwala użytkownikom na personalizację ustawień środowiska. Zatem każdy użytkownik może zdefiniować własne ustawienia systemu, a także innych programów (np. pakietu MS Office). Może określić, jakie skróty będą znajdować się na pulpicie, jak będzie wyglądać Menu Start. Podczas surfowania w Internecie będzie mógł korzystać ze zbudowanego przez siebie systemu Ulubionych adresów.

Te wszystkie dane zapisane są w profilu użytkownika. Wiele programów przechowuje tam konfigurację, a także dane, na których operuje. Np. Outlook Express oprócz konfiguracji zapisuje w profilu foldery z listami i książkę adresową.

Istnieją trzy rodzaje profili użytkownika:

- ***Lokalny profil użytkownika*** zostaje utworzony automatycznie po pierwszym zalogowaniu użytkownika w komputerze i zapisany na lokalnym dysku systemowym w folderze ***Documents and Settings***. Zmiany lokalnego profilu dotyczą tylko komputera, na którym profil występuje.
- ***Mobilny profil użytkownika*** zostaje utworzony przez administratora i zapisany na serwerze sieciowym. Jest on dostępny na każdym komputerze w sieci. W przypadku zmian dokonanych w profilach mobilnych, informacje przechowywane na serwerze, podlegają automatycznej aktualizacji w momencie wylogowania użytkownika. W chwili logowania profil jest pobierany z serwera.
- ***Obowiązkowy profil użytkownika*** przechowywany jest na serwerze sieciowym i zostaje załadowany po każdym zalogowaniu użytkownika, ale nie podlega aktualizacji przy wylogowaniu. Zmian profili obowiązkowych mogą dokonać tylko administratorzy. W przypadku niedostępności profilu zalogowanie użytkownika jest niemożliwe.

Na zakładce ***Profil*** można zdefiniować ścieżkę do profilu mobilnego lub obowiązkowego.

2.1.f Skrypty logowania

Skrypt logowania może być plikiem wsadowym (*.bat lub *.cmd), wykonywalnym lub procedurą (VBScript, JavaScript lub Windows Script Host). Skrypty logowania są często używane do konfigurowania środowiska użytkownika, zasobów sieciowych lub do automatycznego wykonywania poleceń administratora np. aktualizacja baz antywirusowych.

2.1.g Folder macierzysty

Jest to folder przeznaczony na dane użytkownika. Zazwyczaj jest to folder sieciowy, który można przypisać od odpowiedniej literki dysku. Folder taki może być współdzielony przez kilku użytkowników.

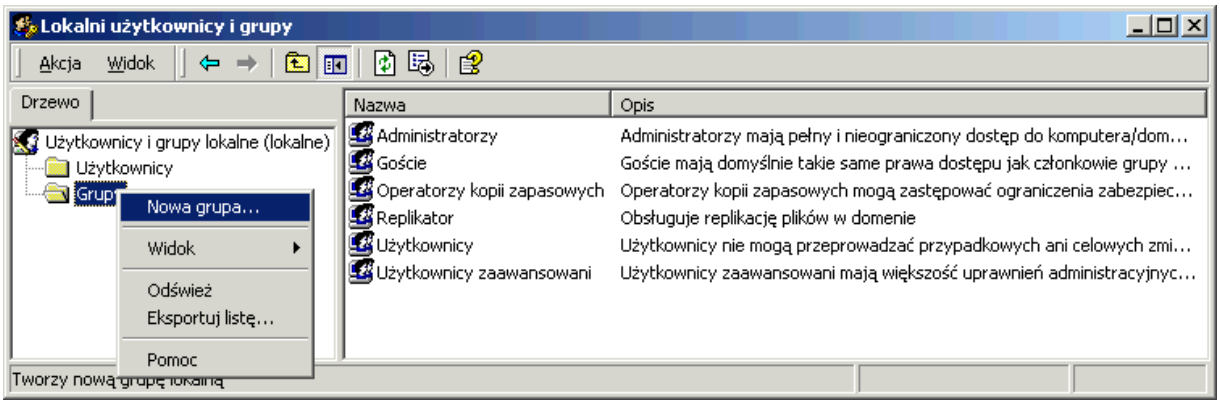
Zadanie 2.1.b – Zarządzanie kontami użytkowników

1. Wymuś na użytkowniku ***jkowalski*** zmianę hasła przy następnym zalogowaniu.
2. Zaloguj się na konto ***jkowalski*** i ustaw hasło na ***jk309***.
3. Utwórz konto ***publiczny*** (w grupie użytkownicy) z pustym hasłem, ustaw opcje tak, aby użytkownik nie mógł zmienić hasła i aby hasło nigdy nie wygasło.
4. Zaloguj się na konto ***publiczny*** i sprawdź, czy użytkownik może zmienić hasło. Uwaga: aby zmienić własne hasło należy nacisnąć ***Ctrl+Alt+Del***, a następnie kliknąć na przycisk ***Zmień hasło***.
5. Wyłącz konto ***apawlak*** sprawdź, czy konto jest zablokowane.

2.1.h Zarządzanie grupami

Aby ułatwić administrację systememu, użytkownicy powinni być łączeni w grupy, którym udostępniane są zasoby i nadawane prawa. Jeżeli użytkownik należy do kilku grup, otrzymuje on prawa wszystkich grup i dostęp do zasobów udostępnionych grupom, do których należy.

Aby założyć nową grupę, należy wybrać ***Zawansowane*** ustawienia kont i z lewej strony okna prawym przyciskiem myszy kliknąć na ***Grupy***, następnie wybrać opcję ***Nowa grupa***.



Rys. 2.5 Zarządzanie grupami

Kolejny krok, to podanie unikalnej ***Nazwy grupy*** (grupa nie może nazywać się tak samo jak użytkownik), opcjonalnego ***Opisu*** i określenie przynależności do grupy, korzystając z przycisków ***Dodaj*** i ***Usuń***.

Aby zmienić przynależność do grup, wystarczy kliknąć dwukrotnie na wybranej grupie i skorzystać z przycisków ***Dodaj, Usuń***.

Zadanie 2.1.c – Zarządzanie kontami grup

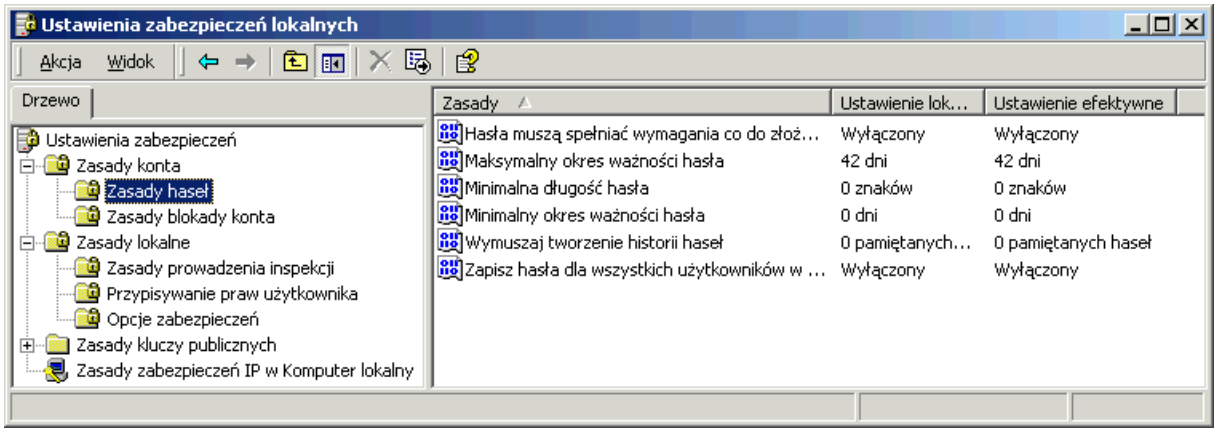
1. Utwórz grupę ***Dyrekcja*** i przypisz do niej konto ***jkowalski***.
2. Utwórz grupę ***Sekretariat*** i przypisz do niej konto ***anowak***.
3. Utwórz grupę ***Księgowość*** i przypisz do niej konto ***tkargul***.

2.2 Zabezpieczenia

2.2.a Wstęp

Administrator ma do dyspozycji bogaty zestaw ustawień podnoszących bezpieczeństwo systemu. Może korzystać z ***zasad kont***, do których należą: ***zasady haseł*** i ***zasady blokady kont***. Ma także do dyspozycji ***zasady lokalne***, a w nich ***zasady prowadzenia inspekcji***, ***przypisywanie praw użytkownika***, ***opcje zabezpieczeń***.

Do zabezpieczeń lokalnych można dostać się przez ***Panel sterowania, Narzędzia administracyjne*** i ikonę ***Zasady zabezpieczeń lokalnych.***



Rys. 2.6 Ustawienia zabezpieczeń

2.2.b Zasady konta

Zasady konta pozwalają administratorowi na wymuszenie na użytkownikach stosowania się do procedur dotyczących haseł, zwiększających bezpieczeństwo systemu. A także korzystając z blokady kont, na ochronę kont przed możliwymi atakami.

Poniżej znajduje się zestawienie dostępnych opcji i standardowe ustawienia.

- ***Hasła muszą spełniać wymagania co do złożoności*** - Wyłączony
- ***Maksymalny okres ważności hasła*** - 42 dni
- ***Minimalna długość hasła*** - 0 znaków
- ***Minimalny okres ważności hasła*** - 0 dni
- ***Wymuszaj tworzenie historii haseł*** - 0 pamiętanych haseł
- ***Zapisz hasła dla wszystkich użytkowników w domenie, korzystając z szyfrowania odwracalnego*** - Wyłączony
- ***Czas trwania blokady konta*** - Nie zdefiniowane
- ***Próg blokady konta*** - 0 nieudanych prób zalogowania
- ***Wyzeruj licznik blokady konta po*** - Nie zdefiniowane

Zadanie 2.2.a – Zasady kont

1. Ustaw wygasanie haseł po 90 dniach.
2. Ustaw minimalną długość hasła na 6 znaków.
3. Wymuś pamiętanie 8 haseł.
4. Przestaw zegar do przodu i sprawdź zachowanie się systemu przy zalogowaniu się na konto ***jkowalski*** i ***publiczny***. Nowe hasło dla ***jkowalski*** ustaw na ***jk309n***.
5. Ustaw blokowanie konta po podaniu 5 błędnych haseł i odblokowanie po 30 min.
6. Sprawdź działanie ustawień punktu 5 (wykorzystaj przesunięcie zegara systemowego).

2.2.c Zasady prowadzenia inspekcji

Inspekcja w systemie Windows NT jest stosowana do śledzenia działań użytkowników oraz wielu zdarzeń systemowych w sieci. Inspekcja pozwala określić, jakie działania lub zdarzenia będą zapisywane w dzienniku zdarzeń zabezpieczeń. Można analizować powodzenia i/lub porażki zdarzeń. Śledzenie powodzenia może dostarczyć informacji o częstotliwości uzyskania dostępu do określonych plików lub drukarek. Informacje te można wykorzystać do planowania zasobów. Śledzenie porażek zdarzeń będzie ostrzegało przed możliwością naruszenia bezpieczeństwa.

2.2.d Prawa użytkownika

Kontom grup lub pojedynczych użytkowników można nadać prawo do wykonywania określonych działań. Prawa różnią się od uprawnień. Prawa dotyczą określonych kont (użytkownicy, grupy), a uprawnia określonych obiektów (np. pliki, foldery, drukarki).

Istnieją dwa rodzaje praw: przywileje (uprawniają użytkownika do wykonywania określonych czynności w sieci) i prawa zalogowania (określają sposoby, na jakie użytkownik może zalogować się w systemie).

Czasami prawa zastępują uprawnienia do określonych obiektów, mają one pierwszeństwo nad uprawnieniami, np. prawo odtwarzania plików i katalogów daje dostęp do plików i katalogów mimo braku uprawnień.

Poniżej znajduje się lista ważniejszych przywilejów i praw zalogowania, a także standardowe przypisanie praw.

- ***Analizowanie programów*** (Administratorzy)
- ***Dodawanie stacji roboczych do domeny***
- ***Ładowanie i usuwanie sterowników urządzeń*** (Administratorzy)
- ***Modyfikowanie zmiennych środowiskowych systemu*** (Administratorzy)
- ***Odtwarzanie plików i katalogów*** (Operatorzy kopii zapasowych, Administratorzy)
- ***Przejmowanie własności plików lub innych obiektów*** (Administratorzy)
- ***Tworzenie kopii zapasowych plików i katalogów*** (Operatorzy kopii zapasowych, Administratorzy)
- ***Wymuszanie zamknięcia systemu z systemu zdalnego*** (Administratorzy)
- ***Zamykanie systemu*** (Użytkownicy, Użytkownicy zaawansowani, Operatorzy kopii zapasowych, Administratorzy)
- ***Zarządzanie inspekcją i dziennikiem zabezpieczeń*** (Administratorzy)
- ***Zmiana czasu systemowego*** (Użytkownicy zaawansowani, Administratorzy)
- ***Zwiększanie kwot*** (Administratorzy)

- ***Logowanie lokalne*** (Gość, Użytkownicy, Użytkownicy zaawansowani, Operatorzy kopii zapasowych, Administratorzy)
- ***Odmowa dostępu do tego komputera z sieci***
- ***Odmowa logowania lokalnego***
- ***Uzyskiwanie dostępu do tego komputera z sieci*** (Wszyscy, Użytkownicy, Użytkownicy zaawansowani, Operatorzy kopii zapasowych, Administratorzy)

2.2.e Opcje zabezpieczeń

Administrator ma do dyspozycji także dodatkowe ustawienia zabezpieczeń znajdujące się w ***Opcjach zabezpieczeń.*** Poniżej znajduje się lista ważniejszych opcji z domyślnymi ustawieniami.

- ***Konsola odzyskiwania: zezwól na automatyczne logowanie administracyjne*** (Wyłączony)
- ***Konsola odzyskiwania: zezwól na kopiowanie na dyskietkę oraz dostęp do wszystkich dysków i folderów*** (Włączony)
- ***Monituj użytkownika o zmianę hasła przed jego wygaśnięciem*** (14 Dni)
- ***Nie wyświetlaj nazwy ostatniego użytkownika na ekranie logowania*** (Wyłączony)

- ***Ogranicz dostęp do stacji CD-ROM tylko do użytkownika zalogowanego lokalnie*** (Wyłączony)
- ***Ogranicz dostęp do stacji dyskietek tylko do użytkownika zalogowanego lokalnie*** (Wyłączony)
- ***Okres bezczynności wymagany dla rozłączenia sesji*** (15 min)
- ***Tekst komunikatu dla użytkowników próbujących się zalogować***
- ***Tytuł komunikatu dla użytkowników próbujących się zalogować***
- ***Wyłącz wymaganie naciśnięcia klawiszy CTRL+ALT+DEL dla zalogowania*** (Nie zdefiniowane)
- ***Wyślij niezaszyfrowane hasło w celu nawiązania połączenia z innymi serwerami SMB*** (Wyłączony)
- ***Zachowanie przy instalacji niepodpisanego niesterownika*** (Nie zdefiniowane)
- ***Zachowanie przy instalacji niepodpisanego sterownika*** (Nie zdefiniowane)
- ***Zapobiegaj instalacji sterowników drukarek przez użytkowników*** (Wyłączony)
- ***Zezwalaj na zamknięcie systemu bez konieczności zalogowania*** (Włączony)

Zadanie 2.2.b – Prawa użytkownika i opcje zabezpieczeń

1. Zabierz prawo ***Logowanie lokalne*** grupom **Gość, *Użytkownicy*** i ***Użytkownicy zaawansowani***.
2. Prawo ***Logowanie lokalne*** nadaj grupom ***Dyrekcja, Sekretariat, Księgowość***.
3. Załącz opcję ***Nie wyświetlaj nazwy ostatniego użytkownika na ekranie logowania***.

2.3 Zasady grup

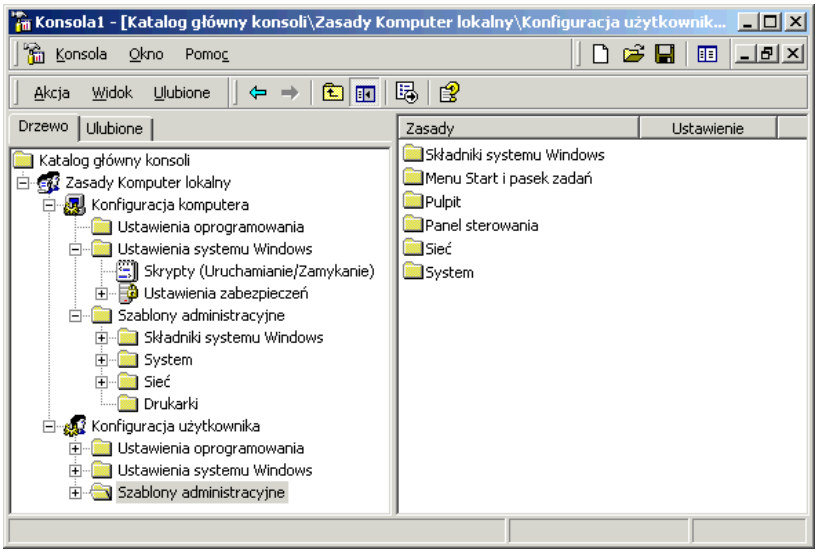
2.3.a Wprowadzenie

Zasady grup umożliwiają wprowadzenie ograniczeń systemu operacyjnego, pulpitu i aplikacji. Najczęściej z zasad grup korzysta się w domenie 2000, a ustawienia globalne wprowadza się na serwerze w Active Directory. Jeżeli nie jest dostępny serwer Active Directory, wówczas zasady grup można ustawiać w obiektach lokalnych. Znajdują się one w ***główny_katalog_systemowy\System32\GroupPolicy***. Dostęp do zasad grup ma administrator z konsoli ***MMC*** i przystawki ***Zasady grup***. Zasady podzielone są na trzy kategorie: ***ustawienia zabezpieczeń*** (opisane w poprzednim rozdziale)***, szablony administracyjne*** i ***skrypty***.

Aby dostać się do zasad grup:

1. Należy uruchomić konsolę ***mmc*** (przez Start - Uruchom).
2. Z menu ***Konsola*** wybrać ***Dodaj/Usuń przystawkę.***
3. Następnie dodać przystawkę ***Zasady grup.***
4. Zatwierdzić ***OK.***

Przystawka ***Zasad grup*** może być wykorzystana do zmiany ustawień zdalnego komputera.



Rys. 2.7 Przystawka Zasady grup

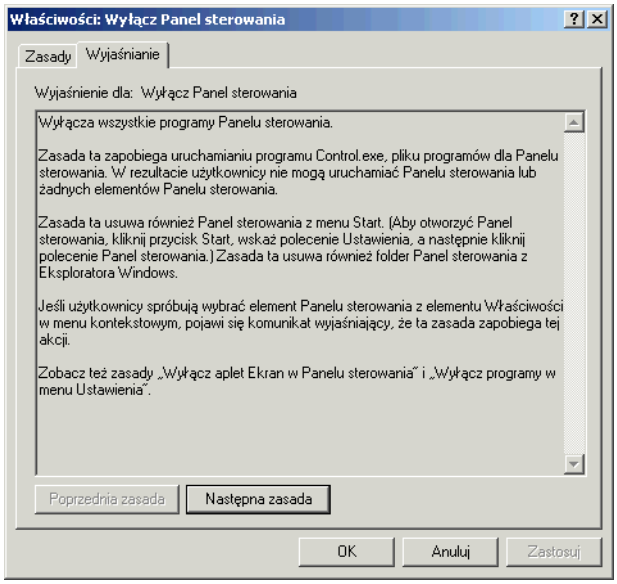
Ustawienia ***Zasad grup*** podzielone są na konfigurację komputera i użytkownika. Jeżeli korzysta się z lokalnych zasad, wówczas ustawienia użytkownika dotyczą wszystkich osób pracujących na danym komputerze, także administratora. Jedyna możliwość wyłączenia zasad dla wybranych kont, to zabronienie odczytu na folder, w którym przechowywane są obiekty zasad ***główny_katalog_systemowy \System32\GroupPolicy.***

Ustawienia zasad grup mogą być zdefiniowane jako ***Włączone***, ***Wyłączone*** lub ***Nie skonfigurowane***.

Jeżeli korzysta się z zasad grupowych domeny, mają one pierwszeństwo przed lokalnymi ustawieniami.

2.3.b Szablony administracyjne

Szablony administracyjne umożliwiają ustawienie ponad 450 typów zachowań systemu operacyjnego. Na zakładce ***Wyjaśnienie*** okna ***Właściwości*** wybranego ustawienia znajduje się dokładny opis.

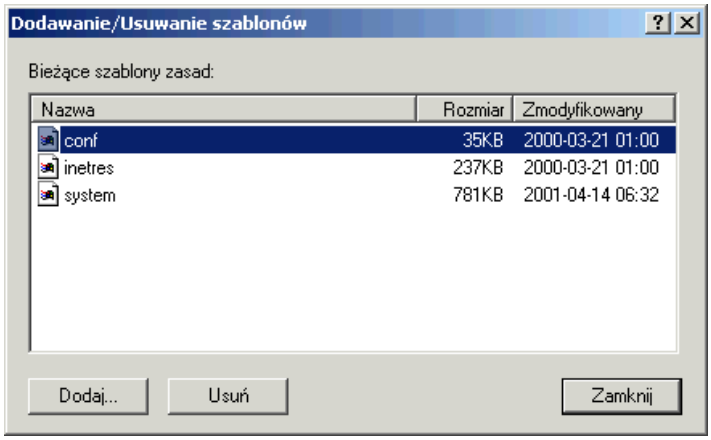


Rys. 2.8 Wyjaśnienie wybranego ustawienia zasad grup

Szablony administracyjne zawierają opcje służące do wymuszania ustawień rejestrowych wpływających na zachowanie się systemu operacyjnego. Zbiór ustawień przechowywany jest w pliku tekstowym z rozszerzeniem ***.adm***. Plik taki zawiera hierarchię definiującą sposób wyświetlania opcji, a także miejsce w rejestrze odpowiadające danemu ustawieniu.

W systemie Windows 2000 znajdują się trzy pliki ***.adm*** – ***system.adm, inetres.adm, conf.adm*** w podkatalogu ***GroupPolicy*** systemu.

Aby dodać nowy szablon wystarczy kliknąć prawym przyciskiem myszy na gałęzi ***Szablony administracyjne*** i wybrać opcję ***Dodaj/Usuń szablony ...***



Rys. 2.9 Dodawanie szablonów administracyjnych

Zdefiniowane ustawienia przechowywane są w plikach ***registry.pol*** w dwóch podkatalogach ***GroupPolicy***. Folder ***Machine*** zawiera ustawienia komputera, folder ***User*** ustawienia użytkownika. Jeżeli administrator zarządzający stacjami Windows 2000, bez serwera 2000, chce wprowadzić identyczne ustawienia, może skopiować te pliki na wszystkie komputery.

2.3.c Skrypty

Skrypt może być plikiem wsadowym (*.bat lub *.cmd), wykonywalnym lub procedurą (VBScript, JavaScript lub Windows Script Host). Skrypty są często używane do konfigurowania środowiska użytkownika, zasobów sieciowych lub do automatycznego wykonywania poleceń administratora np. aktualizacja baz antywirusowych. Za pomocą zasad grup można ustawić skrypty dla komputera wykonywane podczas uruchamiania i/lub zamykania systemu, a także dla użytkownika uruchamiane podczas logowania i/lub wylogowania użytkownika.

Zadanie 2.3 – Lokalne zasady grup

1. Wyłącz funkcję ***Autoodtwarzanie***.
2. Ukryj kartę ***Tło*** właściwości ***Ekranu***.
3. Wyłącz zmianę tapety.
4. Wyłącz aplet panelu sterowania ***Dodaj/Usuń sprzęt (hdwwiz.cpl)***.
5. Wyłącz narzędzia edycji rejestru.
6. Zabroń uruchamiania programu ***mspaint.exe***
7. Sprawdź, czy zmiany zadziałały.

2.4 Uprawnienia do plików i folderów

2.4.a Wprowadzenie

Windows 2000 powinien pracować na dyskach sformatowanych w systemie NTFS. NTFS dostarcza wysoki poziom bezpieczeństwa danych. Każdy plik i folder ma swojego właściciela, każdy plik i folder może mieć przypisaną listę kontroli dostępu (ACL). Uprawnienia NTFS często nazywane są uprawnieniami lokalnymi gdyż chronią lokalne pliki i foldery. Z uprawnień NTFS powinno się korzystać w celu ochrony zasobów przed użytkownikami pracującymi na komputerze, na którym przechowywane są zasoby i użytkownikami zdalnie podłączającymi się do udostępnianych folderów.

Uprawnienia do folderu zawierają takie opcje jak ***Pełna kontrola***, ***Modyfikacja***, ***Zapis i Wykonanie***, ***Wyświetlenie zawartości folderu***, ***Odczyt***, ***Zapis***. Uprawnienia do plików nie zawierają opcji ***Wyświetlenie zawartości folderu***. Każde z tych uprawnień jest logiczną grupą składającą się z uprawnień specjalnych, co przedstawia poniższa tabela.

Uprawnienia specjalne	Pełna kontrola	Modyfikacja	Zapis i wykonanie	Wyświetlenie zawartości folderu	Odczyt	Zapis
Przechodzenie poprzez folder/Wykonanie pliku	**x**	**x**	**x**	**x**		
Wyświetlenie zawartości folderu/Odczyt danych	**x**	**x**	**x**	**x**	**x**	
Odczyt atrybutów	**x**	**x**	**x**	**x**	**x**	
Odczyt rozszerzonych atrybutów	**x**	**x**	**x**	**x**	**x**	
Tworzenie plików/Zapis danych	**x**	**x**				**x**
Tworzenie folderów/ Dołączanie danych	**x**	**x**				**x**
Zapis atrybutów	**x**	**x**				**x**
Zapis rozszerzonych atrybutów	**x**	**x**				**x**
Usuwanie podfolderów i plików	**x**					
Usuwanie	**x**	**x**				
Odczyt uprawnień	**x**	**x**	**x**	**x**	**x**	
Zmień uprawnienia	**x**					
Przejęcie na własność	**x**					

Opcje ***Wyświetlenie zawartości folderu*** oraz ***Zapis i wykonanie*** wydają się mieć takie same uprawnienia specjalne, jednak uprawnienia te są dziedziczone w różny sposób. Uprawnienie ***Wyświetlenie zawartości folderu*** jest dziedziczone jedynie przez foldery a nie przez pliki, natomiast uprawnienie ***Zapis i wykonanie*** jest dziedziczone zarówno przez pliki, jak i przez foldery.

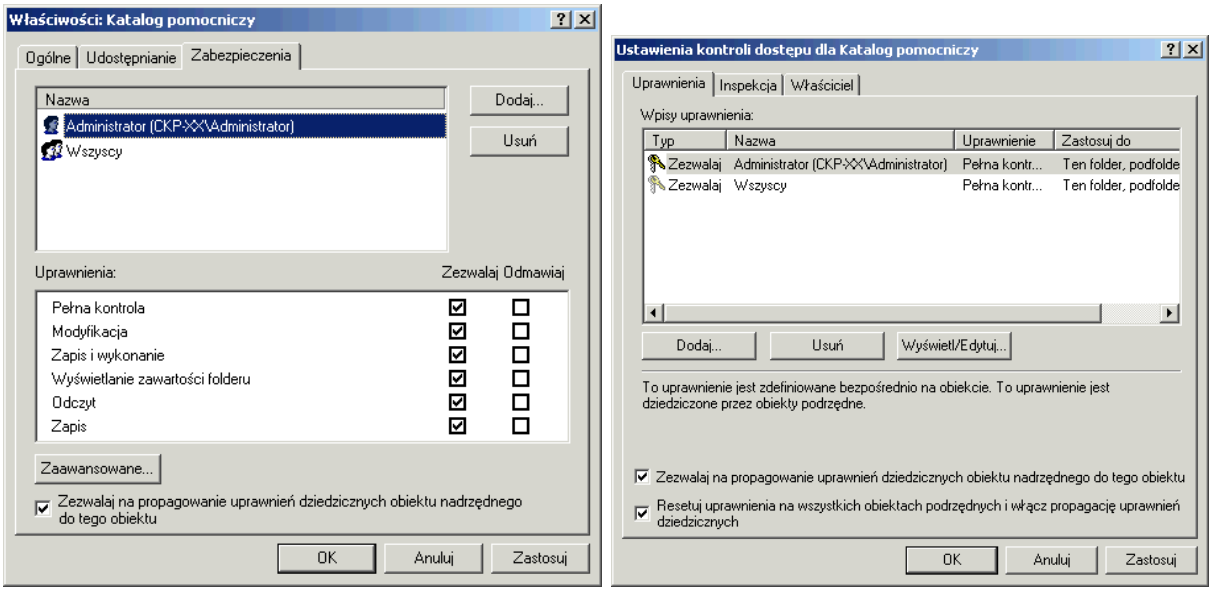
Grupy lub użytkownicy, którym przyznano uprawnienie ***Pełna kontrola*** dla folderu, mogą usuwać z tego folderu dowolne pliki niezależnie od uprawnień chroniących plik.

Poniżej znajduje się dokładny opis uprawnień specjalnych:

- ***Przechodzenie poprzez folder/Wykonanie pliku*** – uprawnienie ***Przechodzenie poprzez folder*** zezwala lub zabrania przechodzenia przez foldery, po to aby dostać się do innych plików lub folderów. Uprawnienie to działa nawet wtedy, gdy użytkownik nie ma uprawnień do folderów, przez które chce przechodzić (dotyczy tylko folderów). Uprawnienie to działa tylko wtedy, gdy grupie lub użytkownikowi nie przyznano prawa ***Pomiń sprawdzanie przechodzenia***. Domyślnie prawo to przyznane jest grupie ***Wszyscy***. Uprawnienie ***Wykonanie pliku*** zezwala lub zabrania uruchamiania plików programu (dotyczy tylko plików).
- ***Wyświetlenie zawartości folderu/Odczyt danych*** – uprawnienie ***Wyświetlenie zawartości folderu*** zezwala lub zabrania przeglądania nazw plików i nazw podfolderów, które znajdują się wewnątrz folderu (dotyczy tylko folderów). Uprawnienie ***Odczyt danych*** zezwala lub zabrania przeglądania danych znajdujących się w pliku (dotyczy tylko plików).
- ***Odczyt atrybutów*** - zezwala lub zabrania przeglądania atrybutów pliku lub folderu, takich jak tylko do odczytu lub obiekt ukryty. Atrybuty są definiowane przez system plików NTFS.
- ***Odczyt rozszerzonych atrybutów*** - zezwala lub zabrania przeglądania rozszerzonych atrybutów plików lub folderów, takich jak archiwizacja, kompresja, szyfrowanie.
- ***Tworzenie plików/Zapis danych*** – uprawnienie ***Tworzenie plików*** zezwala lub zabrania tworzenia plików wewnątrz folderu (dotyczy tylko folderów). Uprawnienie ***Zapis danych*** zezwala lub zabrania wprowadzania zmian do pliku i zastępowania istniejącej zawartości pliku (dotyczy tylko plików).
- ***Tworzenie folderów/Dołączanie danych*** – uprawnienie ***Tworzenie folderów*** zezwala lub zabrania tworzenia folderów wewnątrz folderu (dotyczy tylko folderów). Uprawnienie ***Dołączanie danych*** zezwala lub zabrania wprowadzania zmian na końcu pliku, nie zmieniając, nie usuwając i nie zastępując istniejących danych (dotyczy tylko plików).
- ***Zapis atrybutów*** - zezwala lub zabrania zmieniania atrybutów pliku lub folderu, takich jak ***tylko do odczytu***, czy ***obiekt ukryty***. Atrybuty są definiowane przez system plików NTFS.
- ***Zapis rozszerzonych atrybutów*** - zezwala lub zabrania zmieniania rozszerzonych atrybutów pliku lub folderu. Rozszerzone atrybuty są definiowane przez programy i mogą być różne w zależności od programu.
- ***Usuwanie podfolderów i plików*** - zezwala lub zabrania usuwania podfolderów i plików, nawet wtedy gdy użytkownikowi nie zostało przyznane uprawnienie Usuwanie, które dotyczy tego podfolderu lub pliku.
- ***Usuwanie -*** zezwala lub zabrania usuwania pliku lub folderu. Jeśli użytkownikowi nie przyznano uprawnienia ***Usuń*** do pliku lub folderu, to może on usunąć ten plik lub folder, jeśli przyznano mu uprawnienie ***Usuń podfoldery i pliki*** do folderu nadrzędnego.
- ***Odczyt uprawnień*** - zezwala lub zabrania odczytywania uprawnień do pliku lub folderu.
- ***Zmień uprawnienia*** - zezwala lub zabrania zmieniania uprawnień do pliku lub folderu.
- ***Przejęcie na własność*** - zezwala lub zabrania przejmowanie na własność pliku lub folderu. Właściciel pliku lub folderu może zawsze zmienić uprawnienia, niezależnie od istniejących już uprawnień, które chronią ten plik lub folder.

2.4.b Zmiana uprawnień

Uprawnienia można zmieniać klikając prawym przyciskiem myszy na pliku lub folderze i wybierając ***Właściwości,*** następnie zakładkę ***Zabezpieczenia***. Przy pomocy przycisków ***Dodaj i Usuń*** można zarządzać listą kontroli dostępu. W dolnej części okna, w sekcji ***Uprawnienia*** można zezwolić lub odmówić wybrane uprawnienie. Jeżeli użytkownik należy do kilku grup, to dostaje sumę uprawnień wszystkich grup. Należy jednak pamiętać, iż uprawnienie ***Odmawiaj*** ma wyższy priorytet niż ***Zezwalaj***.



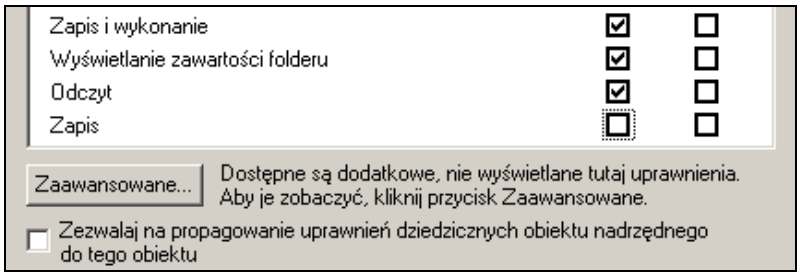
Rys. 2.10 Ustawienia kontroli dostępu do folderu

Domyślnie system przyznaje uprawnienie ***Zapis i wykonanie***, ***Wyświetlenie zawartości folderu***, ***Odczyt***. Uprawnienie ***Zapis i wykonanie*** nie zezwala na zapis. Aby istniała możliwość zapisu, dodatkowo musi być załączone uprawnienie ***Zapis***. Uprawnienie ***Zapis i wykonanie*** daje możliwość odczytu i wykonania plików, zatem powinno ono nazywać się ***Odczyt i wykonanie***. Uprawnienie ***Odczyt*** nie daje możliwości uruchomienia pliku.

Domyślnie nowo tworzone katalogi i pliki mają ustawioną opcję ***Zezwalaj na propagowanie uprawnień dziedzicznych obiektów nadrzędnych do tego obiektu.*** Oznacza to, iż uprawnienia są dziedziczone po folderze wyższego poziomu. Dziedziczenie to można jednak wyłączyć. Należy wówczas określić, czy system ma skopiować uprawnienia, czy usunąć.

Dodatkowo użytkownik ma możliwość wybrania opcji ***Resetuj ustawienia na wszystkich obiektach podrzędnych i włącz propagację uprawnień dziedziczonych***. Ustawienie to dostępne jest po wybraniu przycisku ***Zaawansowane***.

Folder utworzony na dysku (C:) dziedziczy uprawnienia po dysku (C:). Dysk (C:) tak jak każdy wolumin domyślnie udostępniony jest grupie ***Wszyscy*** z ***pełna kontrolą***. Grupa ***Wszyscy*** jest specjalną grupą obejmująca wszystkich użytkowników, nawet tych, którzy nie posiadają konta. Chcąc zabezpieczyć nowo utworzony folder, grupie ***Wszyscy*** trzeba zabrać uprawnienia. Przy tej operacji należy pamiętać, że jeśli administratora nie będzie na liście uprawnień, to nie będzie miał on dostępu do folderu. Zatem zawsze do listy uprawnień należy dodać grupę ***Administratorzy*** z pełną kontrolą.

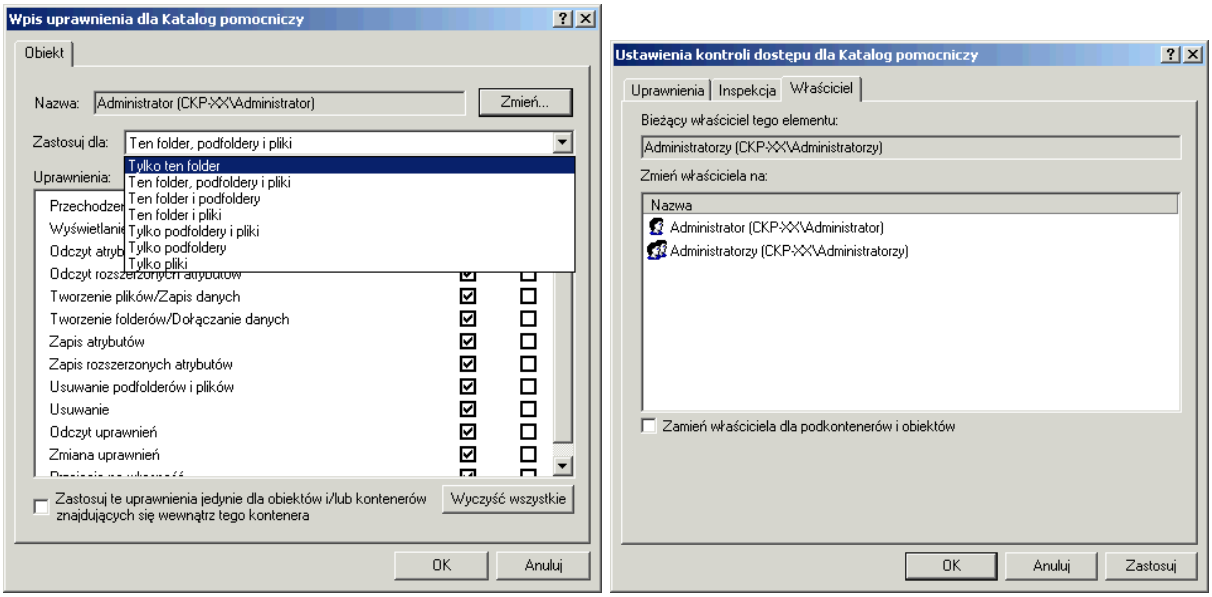


Rys. 2.11 Informacja o dodatkowych uprawnieniach specjalnych

Przy zmianie uprawnień, warto zwrócić uwagę na komunikat ***Dostępne są dodatkowe, nie wyświetlone tutaj uprawnienia,*** pojawiający się przy przycisku ***Zaawansowane.*** Jeżeli np. użytkownik ma uprawnienie ***Pełna kontrola*** i zabierze się uprawnienie ***Zapis***, to pozostaną zaznaczone uprawnienia ***Zapis i wykonanie, Wyświetlenie zawartości folderu i Odczyt.*** W tym przypadku użytkownik będzie posiadał dodatkowe uprawnienia specjalne.

Jeżeli zachodzi potrzeba modyfikacji uprawnień specjalnych, to w opcjach ***Zaawansowanych,*** po wybraniu przycisku ***Wyświetl/Edytuj,*** użytkownik może je zmienić. Podczas tej operacji użytkownik określa, do jakich elementów system ma zastosować zmiany. Można wybrać:

- Tylko ten folder,
- Ten folder, podfoldery i pliki,
- Ten folder i podfolder,
- Ten folder i pliki,
- Tylko podfoldery i pliki,
- Tylko podfoldery,
- Tylko pliki.



Rys. 2.12 Zmiana uprawnień specjalnych i właściciela

W zaawansowanych ustawieniach kontroli dostępu na zakładce ***Właściciel,*** istnieje możliwość zmiany właściciela pliku lub folderu, a po wybraniu opcji ***Zmień właściciela dla podkontenerów i obiektów*** także do podkatalogów i wszystkich plików w nich występujących. Należy pamiętać, iż właściciel zawsze może zmienić uprawnienia, niezależnie od istniejących już uprawnień, które chronią plik lub folder.

Na zakładce ***Inspekcja*** administrator może załączyć tworzenie dzienników dostępu do plików lub folderów wybranych użytkowników lub grup.

Zadanie 2.4.a – Uprawnienia do plików i folderów

1. Na dysku C: utwórz katalogi:
   - <***Dyrekcja***>
   - <***Sekretariat***>
   - <***Księgowość***>
2. Utworzone foldery udostępnij z uprawnieniem ***Modyfikacja*** odpowiednim grupom:
   - folder <***Dyrekcja***> grupie ***Dyrekcja***,
   - folder <***Sekretariat***> grupie ***Sekretariat***,
   - folder <***Księgowość***> grupie ***Księgowość***.

   UWAGA: nie zapomnij o usunięciu z listy uprawnień grupy ***Wszyscy*** i przypisaniu uprawnienia ***Pełna kontrola*** grupie ***Administratorzy***.
3. Dodatkowo grupa ***Dyrekcja*** ma mieć uprawnienie ***Modyfikacja*** do wszystkich folderów.
4. Grupa ***Księgowość*** uprawnienia: ***Zapis i wykonanie, Wyświetlenie zawartości folderu, Odczyt*** do katalogu ***Sekretariat***.
5. Grupa ***Sekretariat*** uprawnienia: ***Zapis i wykonanie, Wyświetlenie zawartości folderu, Odczyt*** do katalogu ***Księgowość***.
6. Sprawdź, czy dobrze ustawiłeś zabezpieczenia folderów, zaloguj się na użytkowników poszczególnych grup, wykonaj operacje na folderach.
7. Utwórz katalog publiczny <***C:\Publiczny***> i udostępnij go wszystkim użytkownikom (np. grupie ***Użytkownicy uwierzytelnieni***) z uprawnieniem ***Modyfikacja***. Korzystając z tego katalogu użytkownicy sieci będą mogli swobodnie przekazywać sobie dane.

   UWAGA: nie zapomnij o usunięciu z listy uprawnień grupy ***Wszyscy*** i przypisaniu uprawnienia ***Pełna kontrola*** grupie ***Administratorzy***.
8. W katalogu <***C:\Sekretariat***> utwórz podkatalog, a w nim plik. Następnie plik ten skopiuj do katalogu <***C:\Publiczny***>. Przeprowadź analizę uprawnień dostępu.
9. Utwórz folder <***C:\Pomoc***> i wcześniej utworzony plik przenieś do tego katalogu. Przeprowadź analizę uprawnień dostępu.
10. Utwórz i sformatuj partycję D:
11. Wykonaj operacje kopiowania i przenoszenia między dyskiem C: i D:. Przeprowadź analizę uprawnień dostępu.
12. Utwórz katalog <***C:\Prace***>, w którym wszyscy ***uwierzytelnieni użytkownicy*** będą mogli zapisywać swoje prace, ale jedynie ***właściciele*** prac będą mogli odczytywać i modyfikować swoje pliki. Inni użytkownicy nie będą mieli dostępu do nie swoich prac (skorzystaj przy tym z grupy ***TWÓRCA WŁAŚCICIEL***). Sprawdź, czy dobrze ustawiłeś uprawnienia.
13. Na folder <***C:\Pomoc***> ustaw uprawnienie ***Pełna kontrola*** dla grupy ***Administratorzy*** i odmów uprawnienie ***Zapis*** dla ***Użytkowników uwierzytelnionych***. Sprawdź, czy ***administrator*** może zapisać plik w folderze <***C:\Pomoc***>.
14. Z konta ***jkowalski*** utwórz katalog <***C:\jkowalski***>, a w nim kilka plików. Ustaw uprawnienia na katalog tak, aby tylko ***jkowalski*** miał uprawnienie ***Pełna kontrola***.
15. Zaloguj się na konto ***Administrator*** i usuń katalog <***C:\jkowalski***> (skorzystaj z operacji przejmowania na własność).

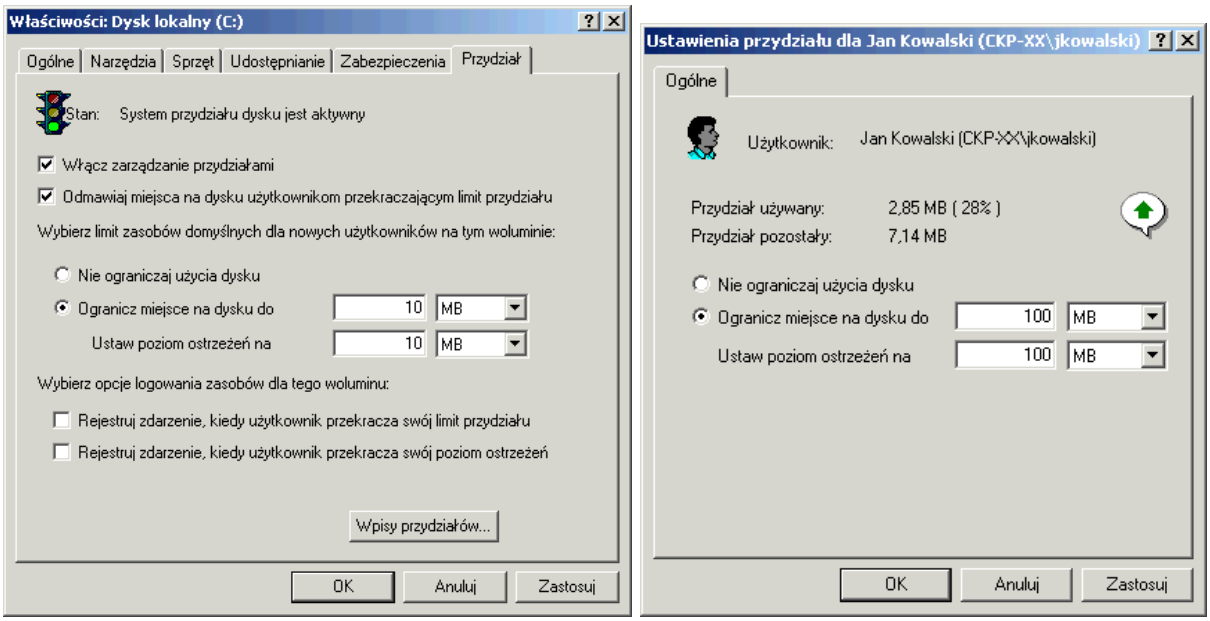
2.4.c *Przydziały dyskowe*

Administrator może załączyć kontrolę wykorzystania przestrzeni dyskowej przez użytkowników. W tym celu, we właściwościach dysku, na zakładce ***Przydział,*** należy załączyć opcję ***Włącz zarządzanie przydziałami***. Aby system pilnował limitu przydziału, dodatkowo należy załączyć opcję ***Odmawiaj miejsca na dysku użytkownikom przekraczającym limit przydziału.*** Przydziały załącza się na każdy dysk z osobna.

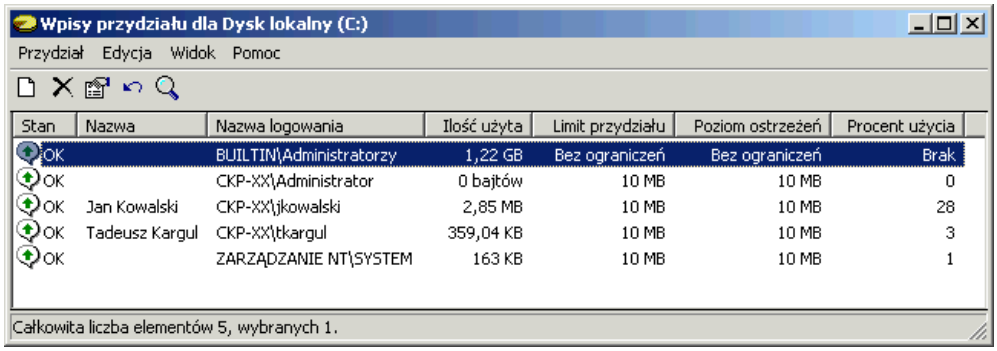
Jeżeli dla wszystkich użytkowników systemu administrator chce ustalić określony przydział, wówczas po wybraniu opcji ***Ogranicz miejsce na dysku do,*** powinien podać wartość domyślną limitu i poziom ostrzegawczy.

Jeżeli zostaną załączone opcje ***Rejestruj zdarzenie,*** wówczas do dziennika systemowego zapisywane jest zdarzenie, w momencie gdy użytkownik osiągnie poziom ostrzegawczy lub limit.

Wybranym użytkownikom, wartość domyślną limitu można zmienić. Wystarczy kliknąć na przycisk ***Wpisy przydziałów*** i wybrać z listy określonego użytkownika. Jeżeli jakiegoś użytkownika nie ma na liście, oznacza to, iż nie posiada on plików w systemie. W tym wypadku można zmienić domyślny limit przydziału przez wybranie z menu ***Przydział*** opcji ***Nowy wpis przydziału***.



Rys. 2.13 Ustawienia przydziałów



Rys. 2.14 Lista przydziałów

Zadanie 2.4.b – Przydziały dyskowe

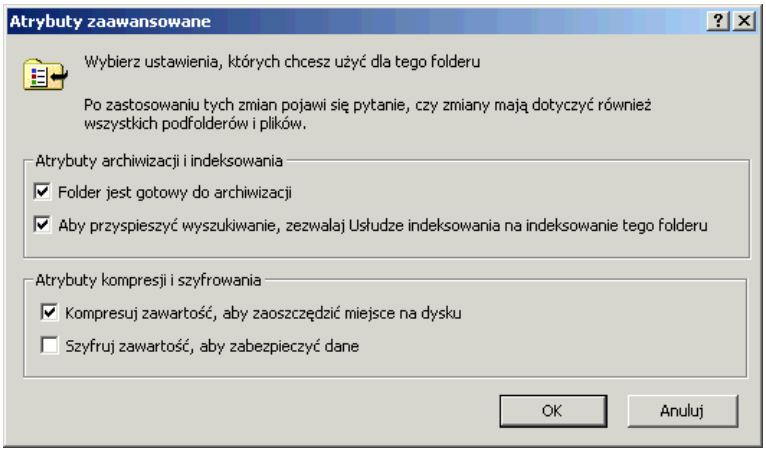
1. Załącz przydziały do dysków C: i D: z blokadą przekroczenia limitu 10MB danych.
2. Użytkownikowi ***jkowalski*** zwiększ limit do 100MB (na dysku C: i D:).
3. Użytkownikowi ***anowak*** zwiększ limit do 50MB (na dysku C: i D:).
4. Po zalogowaniu się na wybranego użytkownika sprawdź, czy system przestrzega zdefiniowanych limitów.

2.4.d Kompresja i szyfrowanie plików i folderów

System plików NTFS daje możliwość załączenia kompresji wybranych plików lub całych folderów. Kompresja i dekompresja wykonywane są automatycznie. Przed zapisem plik jest kompresowany, przed odczytem dekompresowany. Kompresja plików może spowodować spadek wydajności systemu, dlatego też nie powinno załączać się kompresji na często wykorzystywane pliki. System NTFS umożliwia także szyfrowanie wybranych plików. Zaszyfrowany plik może zostać odczytany jedynie przez osobę, która plik zaszyfrowała lub przez administratora.

Jeżeli korzysta się z kompresji, warto w ***Opcjach folderów,*** na zakładce ***Widok*** ustawić ***Wyświetlaj skompresowane pliki i foldery innym kolorem***.

Jeżeli chcesz załączyć kompresję na wybrany plik lub folder, wystarczy wybrać ***Właściwości*** pliku lub folderu i na zakładce ***Ogólne*** kliknąć ***Zaawansowane***. Następnie załączyć opcję ***Kompresuj zawartość, aby zaoszczędzić miejsce na dysku.*** W oknie tym dostępna jest także opcja ***Szyfruj zawartość, aby zabezpieczyć dane***.



Rys. 2.15 Ustawienie atrybutu kompresji

Zadanie 2.4.c – Kompresja plików i folderów

1. Załącz kompresję na folder <***C:\Program files***>, zobacz we właściwościach folderu ile zaoszczędziłeś miejsca, wylicz współczynnik kompresji.
2. Utwórz plik .bmp w folderze <***C:\Program files***>, wylicz współczynnik kompresji.
3. Skopiuj plik utworzony w poprzednim punkcie do folderu <***C:\Publiczny***>. Sprawdź jak system ustawił atrybut kompresji.
4. Przenieś twój plik .bmp z <***C:\Program files***> do <***C:\Prace***>. Sprawdź jak system ustawił atrybut kompresji.
5. Przenieś twój plik .bmp z <***C:\Publiczny***> do <***C:\Program files***>. Sprawdź jak system ustawił atrybut kompresji.

2.5 Literatura

[1] Windows 2000 Professional Resource Kit, Microsoft Press.

[2] http://www.microsoft.com/poland/windows2000/win2000prof/default.asp

2.6 Lista zadań do wykonania i samoocena

Nr zadania	Temat	Ocena (1 – 5 pt.)
2.1.a	Zakładanie kont użytkowników	
2.1.b	Zarządzanie kontami użytkowników	
2.1.c	Zarządzanie kontami grup	
2.2.a	Zasady kont	
2.2.b	Prawa użytkownika i opcje zabezpieczeń	
2.3	Lokalne zasady grup	
2.4.a	Uprawnienia do plików i folderów	
2.4.b	Przydziały dyskowe	
2.4.c	Kompresja plików i folderów	