10.4. Lokalne konta użytkowników i grup

Konto użytkownika to zbiór zasobów i uprawnień w ramach danego systemu, które są przypisane konkretnemu użytkownikowi. We współczesnych systemach operacyjnych konta mają unikatową nazwę (login) i hasło. Proces autoryzacji w systemie, zwykle wymagający podania nazwy konta i hasła, nazywa się **logowaniem**.

W systemach operacyjnych Windows rozróżniamy trzy podstawowe rodzaje kont:

- **konta standardowe** – przeznaczone do codziennego korzystania z komputera;
- **konta administratora** – udostępniają najszerszy zakres kontroli nad komputerem i należy z nich korzystać tylko wtedy, gdy jest to konieczne;
- **konta gości** – przeznaczone przede wszystkim dla osób, które potrzebują tymczasowego dostępu do komputera.

Przy tworzeniu nowego konta użytkownika zostaje przypisany mu jeden z dwóch typów: administrator komputera lub użytkownik standardowy. Gdy tworzymy konto za pomocą apletu **Konta użytkowników** z panelu sterowania, musimy podjąć decyzję, jaki będzie jego typ. Gdy używamy konsoli **Zarządzanie komputerem**, konto takie jest automatycznie przypisane do grupy **Użytkownicy**, co oznacza, że ma ograniczenia.

Użytkownik standardowy ma następujące prawa:

- zmiana własnego obrazu skojarzonego z kontem użytkownika;
- tworzenie, zmiana lub usuwanie własnego hasła;
- zmiana ustawień systemowych, które nie dotyczą innych użytkowników ani zabezpieczeń komputera.

Administrator komputera ma następujące prawa do zarządzania komputerem:

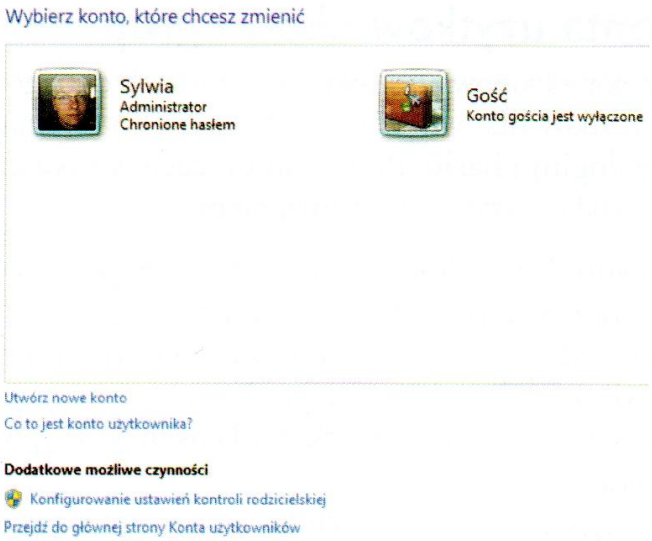
- instalowanie oprogramowania i sprzętu;
- tworzenie, zmiana i usuwanie kont innych użytkowników oraz modyfikacja swojego konta;
- wprowadzanie zmian systemowych i zmian w konfiguracji komputera;
- dostęp do wszystkich plików w komputerze.

W zależności od ustawień powiadamiania administratorzy mogą zostać poproszeni o podanie hasła lub o potwierdzenie przed wprowadzeniem zmian dotyczących innych użytkowników.

10.4.1. Zarządzanie kontami użytkowników – panel sterowania

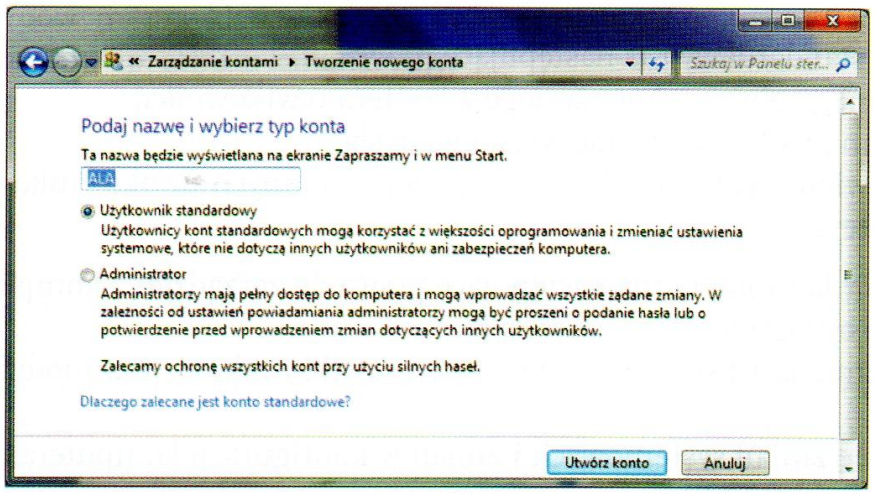
Podczas instalacji Windowsa powstaje pierwsze lokalne konto użytkownika – **Administrator**. W trakcie instalacji użytkownik podaje hasło dla tego konta. Kolejne konta możemy utworzyć zaraz po instalacji. Kreator proponuje nam założenie kont dla użytkowników i możemy to zrobić, jeśli przewidujemy, kto będzie korzystał z komputera. Konta utworzone w ten sposób otrzymują uprawnienia administratora komputera i puste hasło.

Uprawnienia administratora, a więc maksymalne prawa i puste hasło, to niebezpieczna metoda tworzenia kont użytkowników standardowych. Konta te należy wtedy jak najszybciej zmienić na konta z ograniczeniami. Możemy sprawdzić, jak to działa, logując się na konto użytkownika: **Administrator komputera**. W panelu sterowania wybieramy **Konta użytkowników** i **Zarządzaj innym kontem**, a następnie **Utwórz nowe konto** (rys. 10.12).



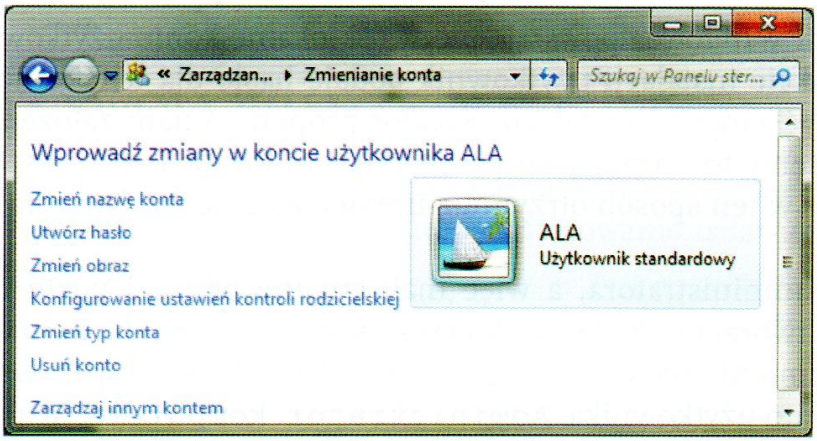
Rys. 10.12. Konta użytkowników

Teraz wybieramy typ konta i jego nazwę, a następnie klikamy **Utwórz konto** (rys. 10.13)



Rys. 10.13. Tworzenie nowego konta

Nowe konto standardowe **ALA** zostało utworzone. Właścicielowi wolno zmienić jego nazwę i obraz, utworzyć hasło itd. Opcje te są dostępne z lewej strony okna (rys. 10.14).



Rys. 10.14. Modyfikacja nowego konta

Aby usunąć konto użytkownika, wystarczy kliknąć opcję **Usuń konto**.

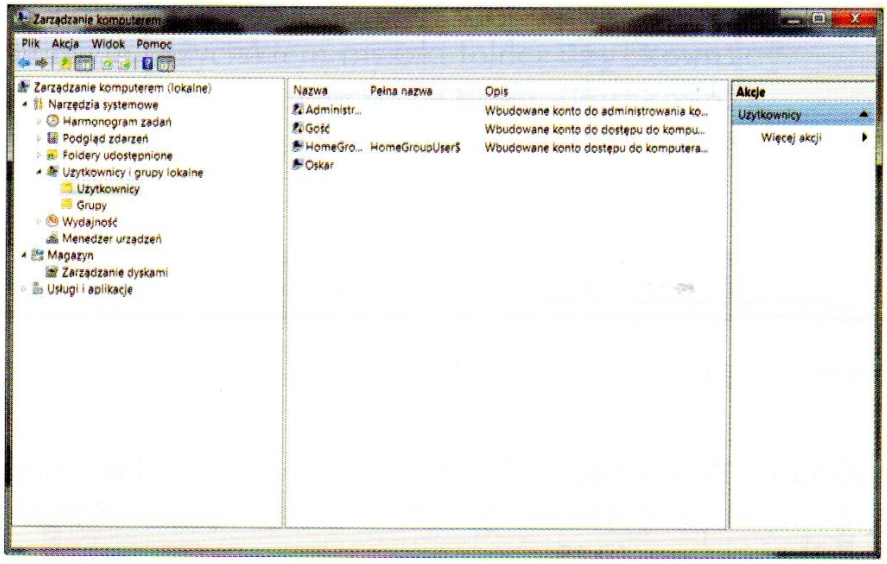
SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Za pomocą panelu sterowania utwórz konto standardowe o nazwie **uczeń**. Dokonaj modyfikacji w ustawieniach innego konta niż to, na którym pracujesz.

10.4.2. Zarządzanie kontami użytkowników – konsola MMC

Kolejny sposób zakładania kont użytkowników lokalnych wykorzystuje konsolę **MMC** (*Microsoft Management Console*). Wysoką funkcjonalność konsoli osiągnięto dzięki zastosowaniu mechanizmu dodawania przystawek. Aby założyć konto użytkownika z wykorzystaniem konsoli MMC, należy wykonać czynności opisane poniżej.

1. Prawym przyciskiem myszy klikamy ikonę **Komputer**.
2. W menu podręcznym wybieramy opcję **Zarządzaj**. Zostanie uruchomiona konsola **Zarządzanie komputerem**.
3. W lewej części okna, na tzw. drzewie konsoli, wybieramy i rozwijamy przystawkę **Użytkownicy i grupy lokalne**.
4. Klikamy opcję **Użytkownicy**, a wtedy w okienku po prawej stronie, w tzw. oknie szczegółów, pojawi się lista kont użytkowników, które już istnieją w komputerze (rys. 10.15).



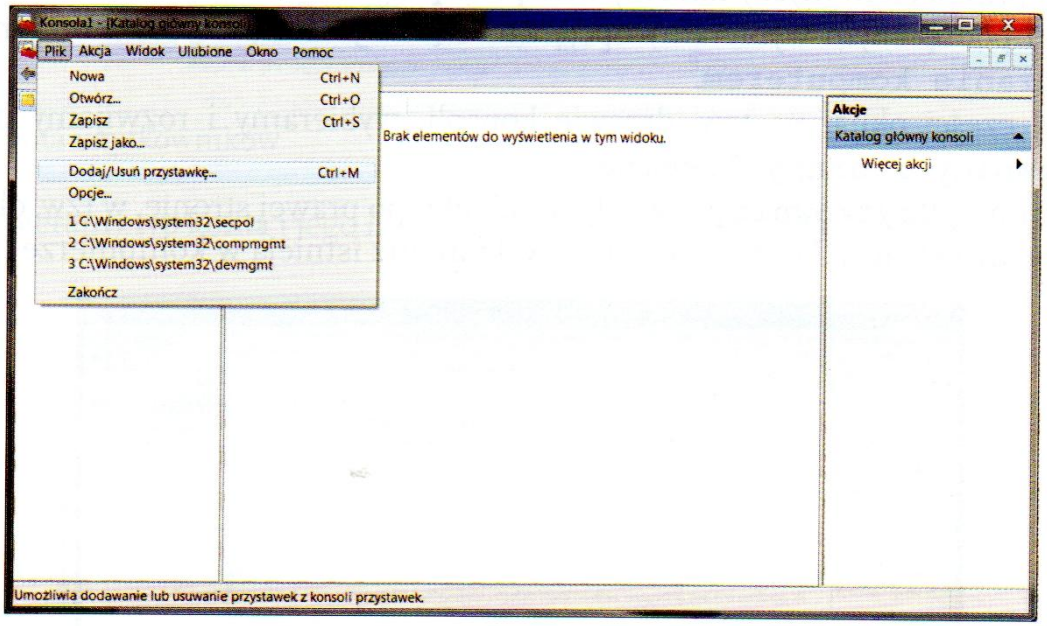
Rys. 10.15. Lista użytkowników komputera lokalnego

5. Klikamy prawym przyciskiem myszy puste pole w oknie szczegółów lub folder **Użytkownicy** w drzewie konsoli. Wówczas pojawi się menu podręczne.
6. W menu podręcznym wybieramy **Nowy użytkownik**.
   - W oknie **Nowy użytkownik** wypełniamy odpowiednie pola: **Nazwa użytkownika** – unikatowa nazwa konta użytkownika używana do jego identyfikacji. Nie może się ona powtórzyć w obrębie lokalnej bazy kont. Nie może też zawierać następujących znaków: „/ \ [ ] : ; | = , + * ? < >. Jej maksymalna długość wynosi 20 znaków.
   - **Pełna nazwa** – nazwa użytkownika wyświetlana w konsoli MMC.
   - **Opis** – opcjonalne miejsce na opis użytkownika lub konta.
   - **Hasło** – tutaj wpisuje się hasło dla konta.
   - **Potwierdź hasło** – tutaj ponownie wpisuje się hasło w celu uniknięcia pomyłki.
7. Następnie konfigurujemy konto, wybiertając dostępne opcje:
   - **Użytkownik musi zmienić hasło przy następnym logowaniu** – wymusza to zmianę hasła podczas pierwszego logowania. Włączenie tej opcji wyklucza dwie następne.
   - **Użytkownik nie może zmienić hasła** – ta opcja odbiera osobie korzystającej z konta możliwość zmiany hasła.

- **Hasło nigdy nie wygasa** – nadpisuje ustawienie Maksymalny okres ważności hasła konfigurowane w **Zasadach grupy**. Określa, że hasło nigdy nie traci ważności.
- **Konto jest wyłączone** – wybór tej opcji wyłącza konto. Wyłączenie konta nie powoduje jednak jego usunięcia. Kiedy konto jest wyłączone, nie można go wykorzystać do logowania.

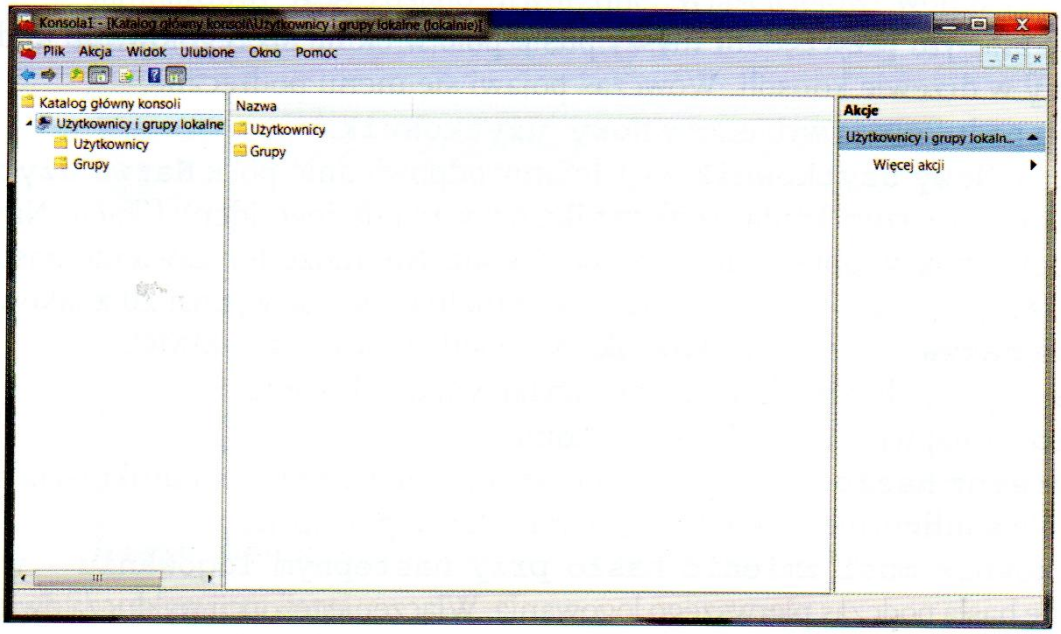
8. Klikamy **Utwórz**.

Inną metodą otwarcia konsoli jest wpisanie polecenia **mmc** w polu **Wyszukaj**. W oknie konsoli wybieramy opcję **Plik / Dodaj/Usuń przystawkę**. Z dostępnych przystawek wybieramy **Użytkownicy i Grupy lokalne** i klikamy **Dodaj** (rys. 10.16).



Rys. 10.16. Dodawanie przystawki w konsoli MMC

Następnie wybieramy **Komputer lokalny**, jeśli to na nim będziemy tworzyć konto użytkownika, a później klikamy **Zamknij** i **OK**. Otworzy się okno **Konsola1** (rys. 10.17), podobne do pokazanego na rys. 10.15.



Ostatnim sposobem zakładania kont użytkowników jest wykorzystanie wiersza polecenia (*Command line*). Ta metoda jest szczególnie przydatna, kiedy musimy założyć kilka kont użytkowników na różnych komputerach. W tym celu można wielokrotnie wydać polecenie tworzenia konta lub napisać odpowiedni plik wsadowy tworzący konta. Wykorzystuje się w nim polecenie **net user**, dzięki któremu można zakładać konta. Poniżej pokazana jest składnia polecenia, które można wykorzystać w pliku wsadowym lub bezpośrednio w wierszu polecenia.

```
net user nazwa_konta haslo_konta_ /add
```

Powyższe polecenie zakłada użytkownika lokalnego

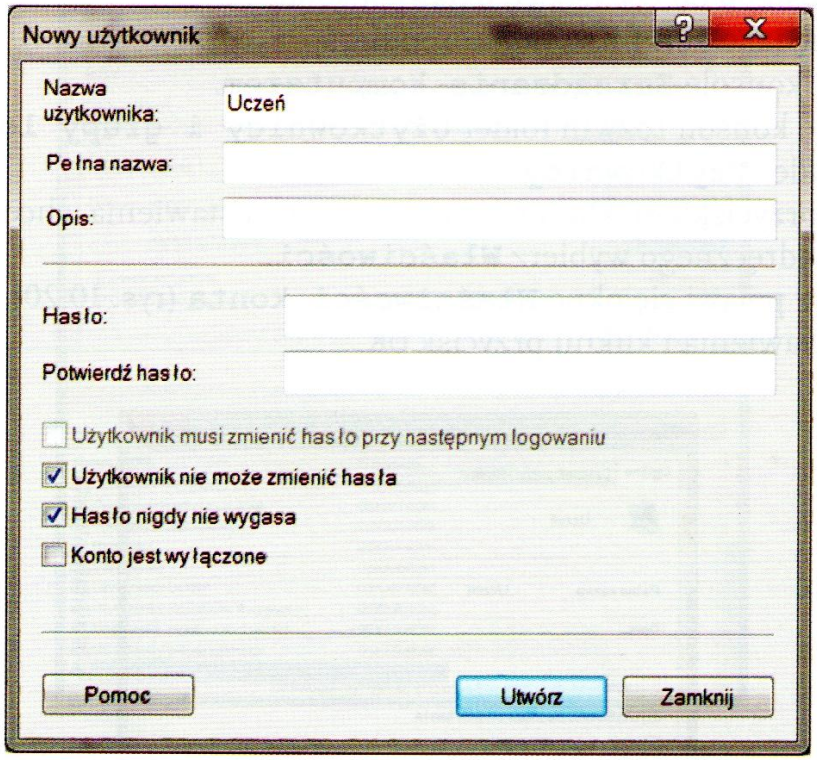
nazwa_konta z hasłem: hasło_konta.

PRZYKŁAD 10.1

Tworzenie nowych kont z ograniczeniami

Aby utworzyć konta nowych użytkowników i uniemożliwić im stworzenie hasła, wykonaj czynności przedstawione poniżej.

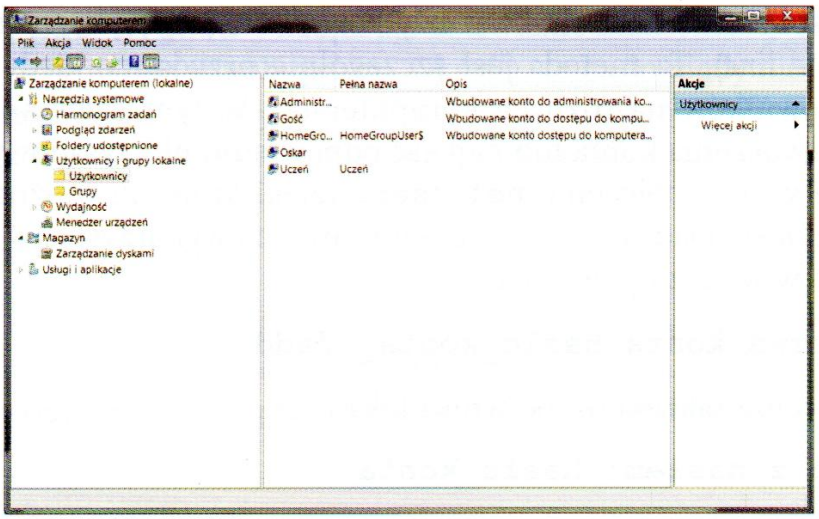
1. Uruchom konsolę **MMC** (*Microsoft Management Console*).
2. Rozwiń menu **Użytkownicy i grupy lokalne**.
3. Kliknij prawym przyciskiem myszki folder **Użytkownicy**.
4. Z menu podręcznego wybierz opcję **Nowy Użytkownik**.
5. Wprowadź nazwę nowego konta użytkownika i ustaw dodatkowe właściwości konta (rys. 10.18).



Rys. 10.18. Tworzenie nowego konta i modyfikacja uprawnień

6. Naciśnij **Utwórz**. Nowy użytkownik został dodany do systemu.
7. Powtórz opisane czynności, żeby stworzyć konto innego użytkownika.
8. Naciśnij **Zamknij**. Okno **Nowy Użytkownik** zostanie zamknięte.

Użytkownik **Uczeń** został dodany do użytkowników na komputerze lokalnym (rys. 10.19).



Rys. 10.19. Nowy użytkownik

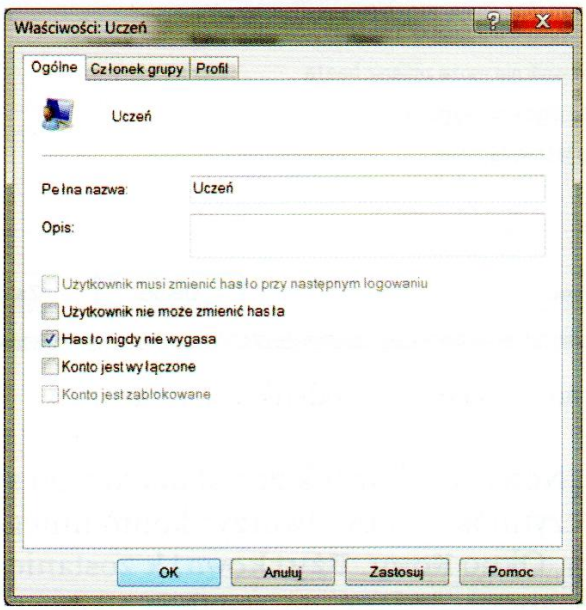
Modyfikowanie kont

Użytkownik z uprawnieniami administratora, tworząc konta dla innych osób, ma dostęp do wielu parametrów kont, w zależności od wybranej metody ich tworzenia. Nawet w metodzie najbardziej zaawansowanej, czyli przez przystawkę **`Użytkownicy i grupy lokalne`**, administrator nie może od razu ustawić wszystkich parametrów. Jest to możliwe dopiero podczas modyfikacji ustawień konta.

PRZYKŁAD 10.2

Uzyskanie dostępu do wszystkich ustawień konta

1. Zaloguj się jako administrator komputera.
2. Uruchom konsolę **`Zarządzanie komputerem`**.
3. W drzewie konsoli rozwiń folder **`Użytkownicy i grupy lokalne`**.
4. Kliknij folder **`Użytkownicy`**.
5. Prawym przyciskiem kliknij konto, którego ustawienia chcesz modyfikować, z menu podręcznego wybierz **`Właściwości`**.
6. Na ekranie pojawi się okno **`Właściwości konta`** (rys. 10.20).
7. Zmień ustawienia i kliknij przycisk **`OK`**.



Rys. 10.20. Okno modyfikacji ustawień konta użytkownika

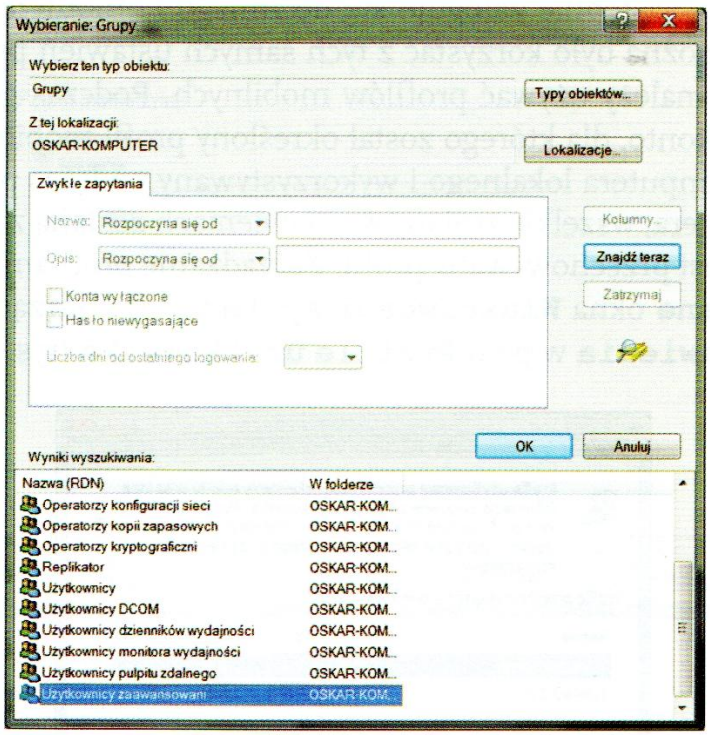
Na karcie **Ogólne** okna **Właściwości konta** znajdują się te same parametry, które opisano wcześniej w procedurze tworzenia konta użytkownika za pomocą konsoli **Zarządzanie komputerem**. Jedyny nowy parametr to **Konto jest zablokowane**, który nie jest włączany manualnie, lecz automatycznie po określeniu w ustawieniach bezpieczeństwa komputera liczby nieudanych prób logowania. Jeżeli konto zostanie zablokowane, tylko osoba mająca uprawnienia administratora komputera może je odblokować. Na karcie **Członek grupy** znajduje się lista grup, do których należy modyfikowane konto.

Grupa użytkowników powala na jednoczesne określenie uprawnień lub właściwości dla większej liczby kont. Każdy użytkownik może być członkiem wielu grup, również grupa może być członkiem innej grupy. Nową grupę można utworzyć za pomocą konsoli **mmc** w przystawce **Użytkownicy i grupy lokalne**. Należy kliknąć prawym przyciskiem myszki folder **Grupy** i z menu podręcznego wybrać opcję **Nowa grupa**. W oknie wprowadzić nazwę nowej grupy, ustawić dodatkowe właściwości i kliknąć przycisk **Utwórz**. Po utworzeniu grupy można przypisać do niej członków.

PRZYKŁAD 10.3

Dodawanie konta do nowej grupy

1. Na karcie **Członek grupy** kliknij przycisk **Dodaj**.
2. Jeśli znasz nazwę grupy, do której chcesz dodać konto, wpisz ją w pole tekstowe **Wprowadź nazwy obiektów do wybrania** (przykłady) i kliknij **Sprawdź nazwy**. Jeśli nie znasz nazwy, kliknij okno **Znajdź teraz** i z list na dole wybierz właściwą grupę (rys. 10.21).



Rys. 10.21. Wybór grupy użytkownika

3. Jeżeli wpisałeś poprawną nazwę grupy, tekst zostanie uzupełniony o nazwę komputera. Na przykład, jeżeli wpisałeś grupę **Administratorzy**, a Twój komputer nazywa się KomputerDom, powinien pojawić się następujący tekst: **KomputerDom\Administratorzy**. Jeżeli nie znasz nazwy grupy, wybierz przycisk **Zaawansowane** i kliknij **Znajdź teraz**. Zobaczysz listę wszystkich dostępnych grup. Zaznacz tę, która Cię interesuje, i kliknij **OK**.

4. Zamknij okno, klikając przycisk **OK**.
5. Jeśli nie wprowadzasz innych modyfikacji konta, kliknij, aby zamknąć **Właściwości konta**.

PRZYKŁAD 10.4

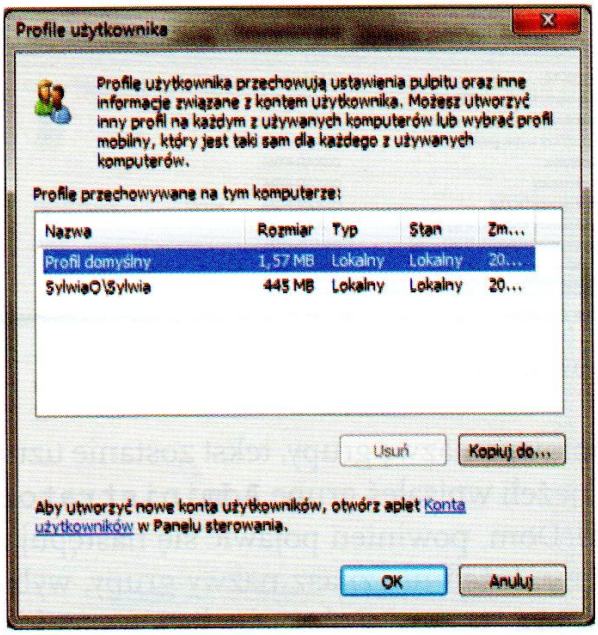
Usuwanie konta z grupy

1. Na karcie **Członek grupy** wybierz grupę, z której chcesz usunąć konto.
2. Kliknij **Usuń**.
3. Kliknij **OK**, aby zamknąć okno **Właściwości konta**.

Ostatnia karta to **Profil**, na której znajdują się parametry dotyczące lokalizacji profilu użytkownika, skryptu logowania i folderu macierzystego.

Domyślnie profile użytkowników Windows są przechowywane na partycji rozruchowej w folderze **Documents and Settings**, w którym każdy użytkownik, choćby raz zalogowany do komputera, posiada swój folder o nazwie zgodnej z nazwą użytkownika. Są to **profile lokalne** przechowywane lokalnie na stacji.

Drugi rodzaj to **profile wędrujące**, inaczej nazywane **mobilnymi** (*Roaming User Profile*), najczęściej wykorzystywane podczas pracy w domenie, lecz nie tylko. Profile mobilne są przechowywane w sieciowym udziale (udostępnionym folderze), do którego użytkownik ma dostęp z każdego komputera pracującego w sieci, podczas gdy profil lokalny jest dostępny wyłącznie podczas pracy na komputerze, gdzie nastąpiło pierwsze logowanie użytkownika i związane z tym utworzenie profilu, który powstaje przy pierwszym logowaniu. Jeżeli użytkownik korzystający z profilu lokalnego zmieni ustawienia zapisywane w profilu na swoim komputerze, a następnie zaloguje się do innego komputera, jego ustawienia nie będą dostępne. Aby można było korzystać z tych samych ustawień profilu przy wszystkich komputerach w sieci, należy używać profilów mobilnych. Podczas gdy użytkownik loguje się do komputera na konto, dla którego został określony profil mobilny, profil ten jest ściągany przez sieć do komputera lokalnego i wykorzystywany podczas pracy. Gdy użytkownik wyloguje się z komputera, wszelkie zmiany w ustawieniach zostaną zapisane w udostępnionym folderze, gdzie jest przechowywany profil. Zarządzanie profilami odbywa się za pomocą karty **Zaawansowane** okna **Właściwości systemu**. Aby zarządzać profilami, należy kliknąć przycisk **Ustawienia** w polu **Profile użytkownika** (rys. 10.22).



Rys. 10.22. Okno Profile użytkownika

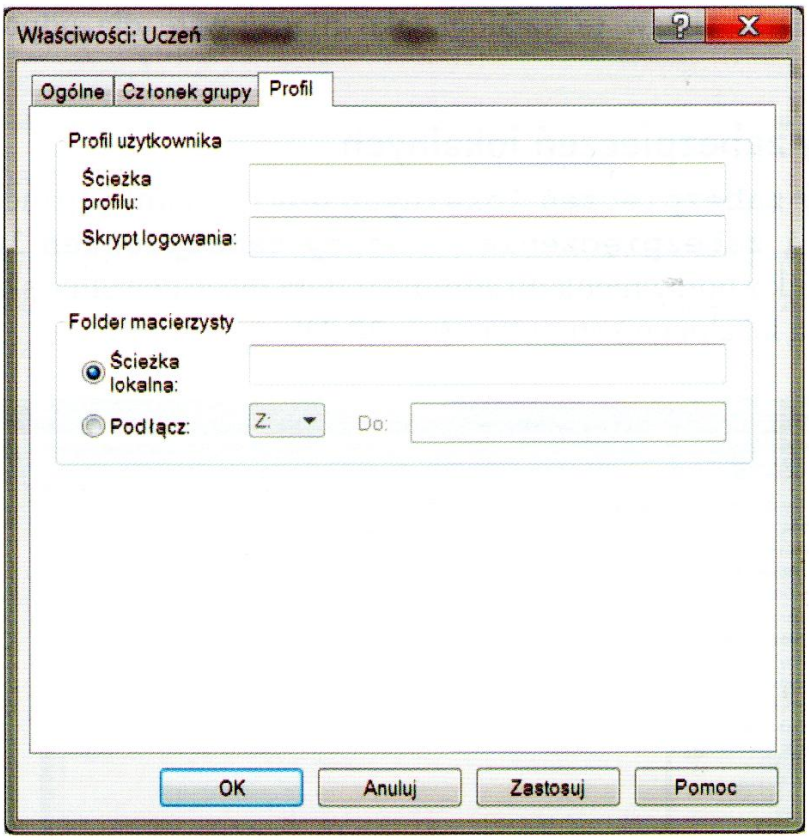
Skrypt logowania to plik wykonywalny, najczęściej napisany w jednym z obsługiwanych języków skryptowych (np. Visual Basic Script Edition), lub plik wsadowy. Skrypt ten jest uruchamiany podczas każdego logowania użytkownika, któremu został przypisany, i może służyć do automatycznego przeprowadzania dodatkowej konfiguracji.

Folder macierzysty to miejsce, gdzie użytkownik przechowuje swoje dane; można go skonfigurować jako ścieżkę lokalną lub podłączyć jako dysk sieciowy. Najczęściej jest wykorzystywana ta druga możliwość, aby użytkownik mógł korzystać ze swojego folderu macierzystego jak z dysku dostępnego (np. z poziomu okna **Komputer**).

PRZYKŁAD 10.5

Zmiana ustawień na karcie Profil

1. W oknie **Właściwości** kliknij kartę **Profil**.
2. W polu **Ścieżka profilu** wpisz ścieżkę lokalną lub sieciową ścieżkę UNC (*Universal Naming Convention*) do folderu, w którym będzie przechowywany profil użytkownika.
   Przykład: **C:\Profile\Nazwa folderu** lub **\\Serwer\Nazwa_udzialu\nazwa_uzytkownika** (rys. 10.23).



Rys. 10.23. Karta Profil z okna Właściwości użytkownika

Jeżeli nie istnieje folder o podanej nazwie, to zostanie on założony podczas pierwszego logowania użytkownika.

Podczas wpisywania lokalizacji sieciowej należy się upewnić, czy nazwa serwera i nazwa udziału są poprawne. Wszyscy użytkownicy, których profile będą przechowywane w udziale, powinni mieć do niego minimalne uprawnienie **Zapis i wykonanie**. Istnieje możliwość używania zmiennej **%username%** zamiast wpisywania nazwy użytkownika, która może być długa lub skomplikowana. Po potwierdzeniu operacji przyciskiem **OK** lub **Zastosuj** zmienna zostanie automatycznie

zastąpiona nazwą użytkownika. Windows automatycznie nadaje właścicielowi profilu i właścicielowi systemu uprawnienie **Pełna kontrola**. Ma to miejsce wyłącznie na partycji NTFS.

3. W polu **Skrypt logowania** wpisz lokalizację skryptu, który ma być uruchamiany podczas logowania na konto.
4. W polu **Ścieżka lokalna** wpisz ścieżkę do folderu na dysku lokalnym lub wybierz opcję **Podłącz**. Wskaż literę dysku, na którą zostanie zamapowany folder macierzysty, następnie podaj ścieżkę UNC do udziału sieciowego.

Podobnie jak w przypadku profilu można używać zmiennej **%username%**, która działa w ten sam sposób.

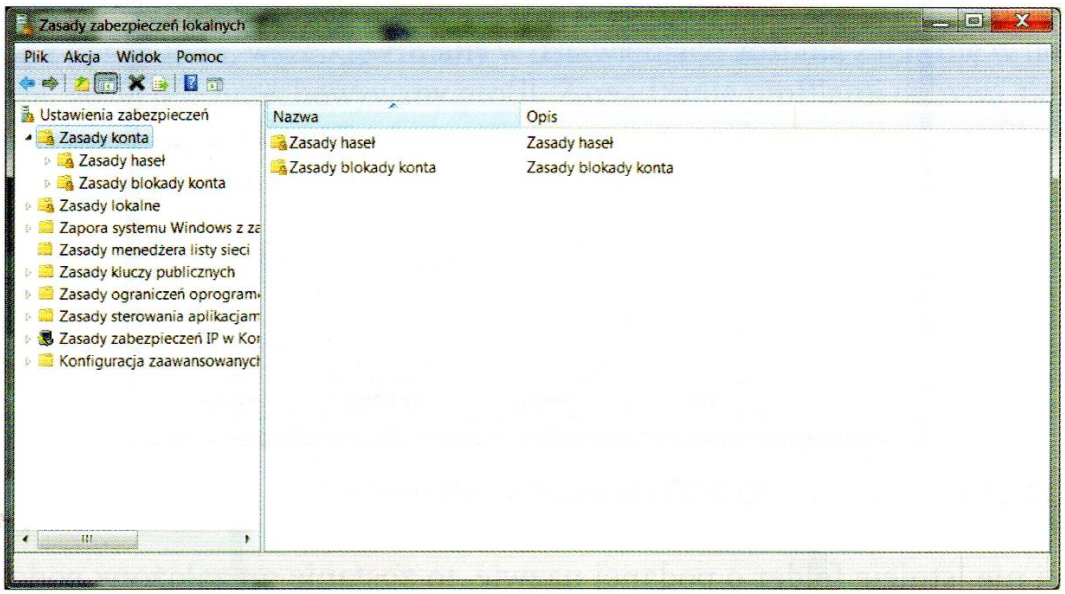
PRZYKŁAD 10.6

Zarządzanie kontami

1. Załóż konta użytkowników: **Mechanik**, **Projektant** – uprawniania użytkownika, **Właściciel** – uprawnienia administratora z hasłem **qwerty123** oraz grupę **Pracownicy**.
2. Przypisz użytkowników **Mechanik** i **Projektant** do grupy **Pracownicy**.
3. Na C:\ załóż folder **Profile**, a w nim podfoldery: **Mechanik**, **Projektant**, **Właściciel**. Ustaw te katalogi jako macierzyste dla odpowiednich użytkowników.

10.4.3. Zasady zabezpieczeń lokalnych

Aplikację **Zasady zabezpieczeń lokalnych** uruchamiamy w panelu sterowania, wybierając **System i zabezpieczenia / Zasady zabezpieczeń lokalnych**. Za jej pomocą użytkownik z uprawnieniami administratora może dowolnie skonfigurować zasady bezpieczeństwa lokalnego komputera (rys. 10.24).



Rys. 10.24. Konsola ustawień zabezpieczeń lokalnych

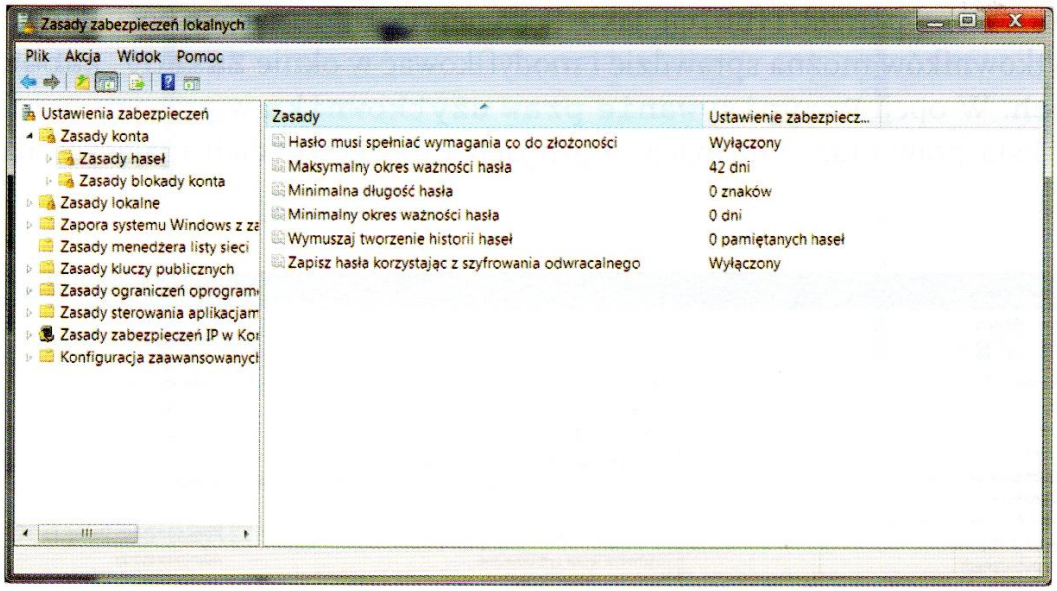
Zasady te podzielono na następujące grupy, które widzimy na lewym panelu okna. Należą do nich między innymi:

- **Zasady konta**, do których zalicza się ustawienia blokady kont oraz zasady haseł;
- **Zasady lokalne**, które obejmują zasady inspekcji, opcje zabezpieczeń i ustawienia związane z przypisywaniem praw użytkownikom;

- **Zasady kluczy publicznych**, zawierające ustawienia dotyczące szyfrowania plików;
- **Zasady ograniczeń oprogramowania**, umożliwiające określenie programów, które można będzie uruchamiać na komputerze;
- **Zasady zabezpieczeń IP**, które pozwalają zabezpieczyć komunikację sieciową.

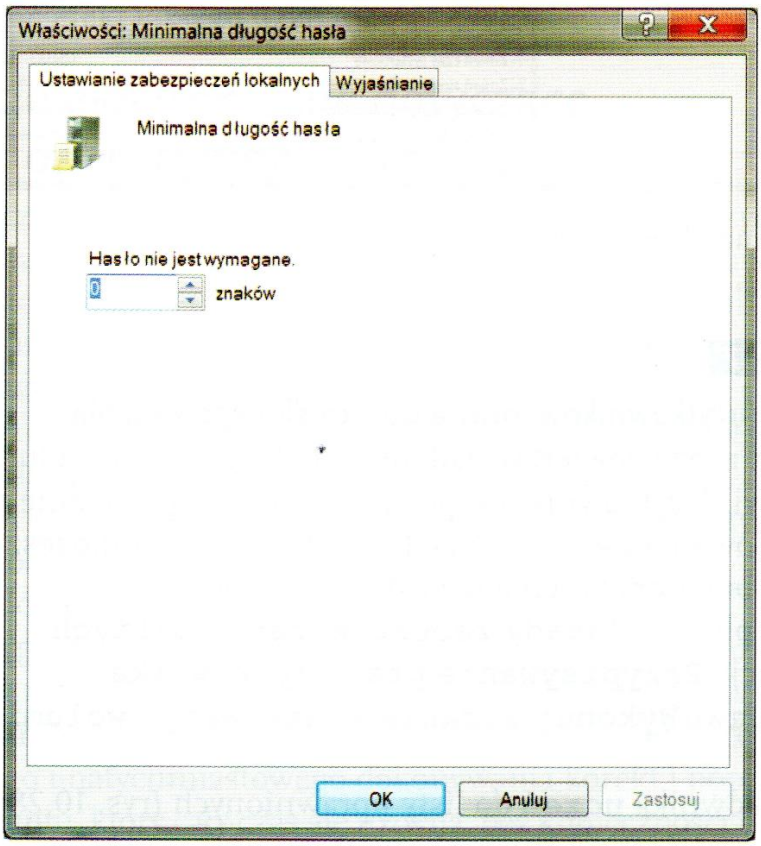
Ograniczenia dotyczące haseł użytkowników

Dla użytkowników można wprowadzić różne ograniczenia związane z hasłami (rys. 10.25).



Rys. 10.25. Zasady haseł

Domyślnie w systemie Windows wymagania złożoności haseł są wyłączone, należy je włączyć przed modyfikacją pozostałych opcji. Aby zmienić opcję, należy ją dwukrotnie kliknąć i wprowadzić nową wartość (rys. 10.26).

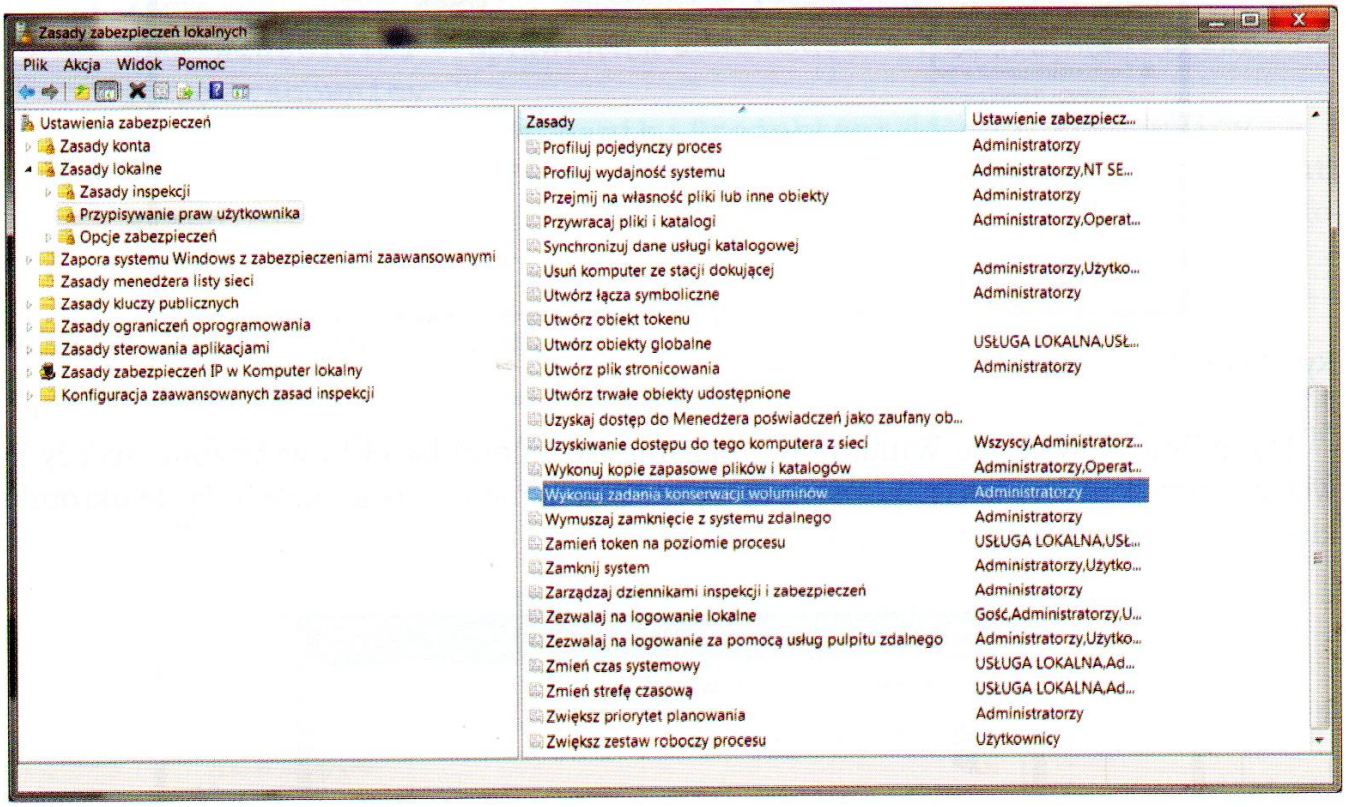


Rys. 10.26. Ustawienia długości hasła

10.4.4. Uprawnienia użytkowników

W systemie Windows poszczególnym grupom i użytkownikom można przydzielić uprawnienia. Można je również przydzielać do udostępnionych zasobów sprzętowych, takich jak drukarki.

Prawa użytkownika określają czynności, jakie może on wykonać w systemie. W systemach, w których jest tylko jeden użytkownik (administrator), ma on wszystkie możliwe prawa. Jeżeli w systemie jest wielu użytkowników, administrator może przydzielać im prawa w zależności od potrzeb i funkcji, jakie będą pełnić. Informacje o posiadanych prawach grup i użytkowników można sprawdzić i modyfikować w oknie **Zasady zabezpieczeń lokalnych**. W opcji **Przypisywanie praw użytkownika** w prawym panelu jest wyświetlana lista praw oraz informacje o grupach i użytkownikach mających dane prawo (rys. 10.27).



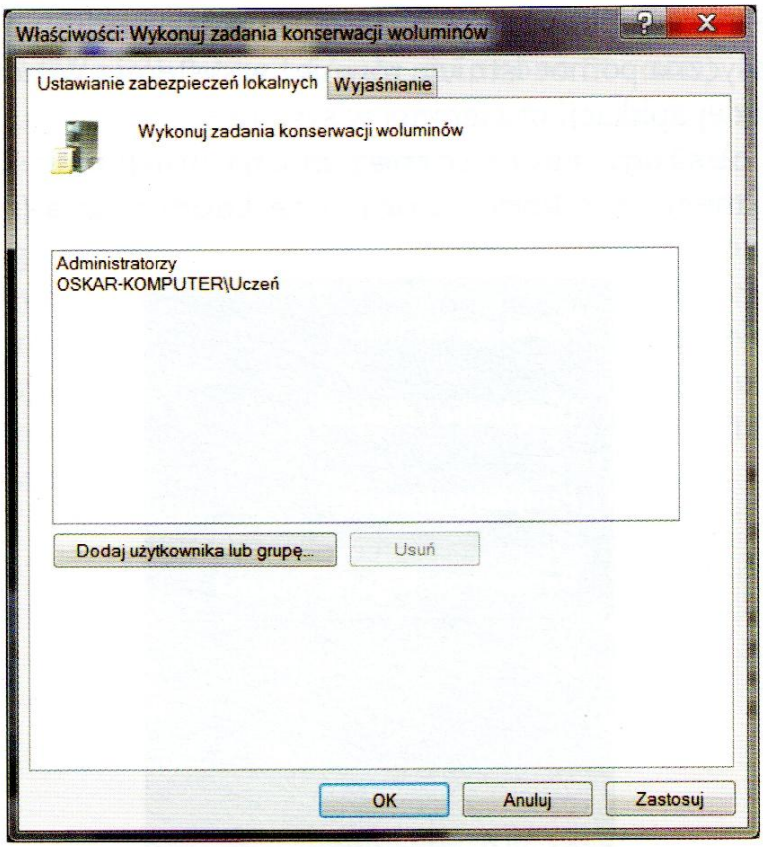
Rys. 10.27. Lista praw użytkowników

PRZYKŁAD 10.7

Przypisywanie użytkownikowi prawa do określonego zadania

Administrator może powierzyć zadanie (np. konserwacji woluminów) wybranemu użytkownikowi. Użytkownik ten powinien mieć odpowiednie prawa umożliwiające realizację powierzonego zadania. Jako administrator możesz przypisać użytkownikowi potrzebne uprawnienia w następujący sposób:

1. Uruchom aplikację **Zasady zabezpieczeń lokalnych**.
2. Wybierz opcję **Przypisywanie praw użytkownika**.
3. Odszukaj prawo **Wykonuj zadania konserwacji woluminów** i kliknij je dwukrotnie.
4. Dodaj użytkownika **uczeń** do listy uprawnionych (rys. 10.28) i kliknij **OK**.



Rys. 10.28. Dodawanie użytkownika do listy uprawnionych

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Utwórz w systemie konto nowego użytkownika. Skonfiguruj tak jego uprawnienia, aby nie mógł się zalogować do systemu. Przetestuj działanie zabezpieczenia.
2. Skonfiguruj politykę haseł użytkowników, tak aby musieli używać haseł o długości co najmniej 5 znaków. Spróbuj zmienić hasło użytkownika na takie, które nie spełnia warunków. Jaki będzie efekt takiego działania?