Instytut Sterowania i Systemów Informatycznych
Uniwersytet Zielonogórski

Systemy operacyjne

Laboratorium

Tworzenie i zarządzanie kontami użytkowników w Windows 7

1 Cel ćwiczenia

Celem ćwiczenia jest opisanie roli i celu tworzenia kont użytkowników oraz omówienie wbudowanych kont użytkowników systemu Windows 7.

2 Podstawowe pojęcia

1. Konta użytkowników

   Konto użytkownika zawiera unikalne dane, które pozwalają na jego uwierzytelnienie oraz umożliwiają użytkownikowi dostęp do zasobów (korzystanie z komputera lokalnego lub zalogowanie się do domeny). Konto użytkownika powinno być zdefiniowane dla każdej osoby, korzystającej regularnie z komputera. Dzięki posiadaniu konta, użytkownik może zalogować się do komputera lub do domeny. Dane, wykorzystane w procesie logowania, służą do kontroli dostępu do zasobów. Istnieją trzy typy kont użytkownika:

   (a) **Lokalne konto użytkownika**. Konto to pozwala na zalogowanie się do określonego komputera i uzyskanie dostępu do zasobów tego komputera. Użytkownik może mieć dostęp również do zasobów innego komputera, jeśli posiada na nim oddzielne konto. Konta użytkowników przechowywane są w bazie SAM (ang. *Security Accounts Manager*) na komputerze lokalnym `C:\Windows\System32\config\SAM`.

   (b) **Domenowe konto użytkownika**. Pozwala na zalogowanie się do domeny i uzyskanie dostępu do zasobów sieciowych. Konta takie można tworzyć na kontrolerze domeny Windows 2008 Server. Użytkownik może uzyskać dostęp do zasobów sieci z dowolnego komputera, posługując się wyłącznie swoją, pojedynczą nazwą użytkownika i hasłem. Konta takie są przechowywane w bazie usługi Active Directory.

   (c) **Wbudowane konta użytkownika**. Pozwalają na wykonywanie zadań administratorskich lub uzyskanie tymczasowego dostępu do zasobów. Istnieją dwa wbudowane konta, których usunięcie nie jest możliwe (aczkolwiek możliwe jest ich wyłączenie): `Administrator` oraz `Gość`. Lokalne konta `Administrator` i `Gość` są przechowywane w bazie SAM, a domenowe w Active Directory. Konta te są tworzone w trakcie instalacji systemu oraz usług katalogowych. Ze względów bezpieczeństwa, konto `Gość` jest wyłączone po instalacji systemu. Jeżeli nie jest wymagany wysoki poziom bezpieczeństwa można je uaktywnić, jednak zalecane jest utworzenie hasła dostępu.

   Rodzaje kont

   Każdy typ konta przyznaje użytkownikowi różne poziomy kontroli nad komputerem. Konto standardowe, to konto do codziennego korzystania z komputera. Konto administratora zapewnia najwyższy poziom kontroli nad komputerem, należy z niego korzystać tylko wtedy, gdy jest to konieczne. Konto gościa jest przeznaczone głównie dla osób potrzebujących tymczasowego dostępu do komputera.

Konto administratora Pozwala instalować oprogramowanie i sprzęt oraz uzyskiwać dostęp do wszystkich plików na komputerze. Administratorzy mogą również wprowadzać zmiany na innych kontach użytkowników. Podczas instalacji systemu Windows będzie konieczne utworzenie konta użytkownika. To konto jest kontem administratora, umożliwiającym skonfigurowanie komputera i zainstalowanie żądanych programów. Po zakończeniu konfigurowania komputera zaleca się korzystanie ze standardowego konta użytkownika do wykonywania codziennych zadań. W tym celu zaleca się założenie nowego konta, które należy do grupy `Użytkownicy` i korzstania z niego na codzień. Korzystanie ze standardowego konta użytkownika (konto należy do grupy `Użytkownicy`) jest bezpieczniejsze niż korzystanie z konta administratora.

Konto gościa To konto użytkownika, który nie dysponuje stałym kontem na komputerze lub w domenie. Umożliwia innym osobom korzystanie z komputera, nie zezwalając jednocześnie na dostęp do prywatnych plików użytkowników. Osoby używające konta gościa nie mogą instalować oprogramowania ani sprzętu, nie mogą zmieniać ustawień ani tworzyć haseł. Konto gościa musi zostać włączone, aby można było z niego korzystać.

Standardowe konto użytkownika Umożliwia korzystanie z większości funkcji komputera. Wprowadzenie zmian dotyczących innych użytkowników lub zabezpieczeń komputera wymaga jednak zgody administratora. Użytkownik korzystający z konta standardowego może używać większości programów zainstalowanych na komputerze, nie może jednak instalować oprogramowania ani sprzętu, usuwać plików niezbędnych do pracy komputera ani zmieniać ustawień dotyczących innych użytkowników tego komputera. W przypadku korzystania z konta standardowego niektóre programy mogą wymagać podania hasła administratora w celu wykonania określonych zadań.

Konwencje nazewnicze kont

Konwencja nazewnicza określa, w jaki sposób konto użytkownika będzie identyfikowane w domenie. Dzięki konwencji nazewniczej łatwiej jest zapamiętać nazwy użytkowników i odnaleźć ich na liście. Dobrą praktyką jest stosowanie zasad nazewniczych, uwzględniających dużą liczbę użytkowników. Konwencja nazewnicza powinna umożliwiać uwzględnienie pracowników o takich samych nazwiskach oraz pozwalać na identyfikację pracowników tymczasowych.

Wskazówki do tworzenia konwencji nazewniczej:

(a) Nazwa konta lokalnego musi być unikalna na komputerze, na którym konto zostało utworzone. Nazwa użytkownika dla konta domenowego musi być unikalna względem całej usługi Active Directory. Pełna nazwa użytkownika musi być unikalna w całej domenie, w której zostało utworzone konto.

(b) Nazwa logowania może zawierać do 20 wielkich i małych znaków. W polu można wpisać więcej znaków, ale Windows 7 rozpoznaje tylko pierwszych 20 z wyjątkiem znaków takich, jak: `"/\[]:;|=,+*?<>@`. Można używać znaków specjalnych i alfanumerycznych, aby nazwa użytkownika była unikalna.

(c) Jeżeli organizacja posiada dużą liczbę użytkowników, to konwencja nazewnicza powinna uwzględniać pracowników o takim samym nazwisku. Przykładowo, można w nazwie konta używać imienia i pierwszej litery nazwiska, a w razie konieczności dodawanie kolejnych liter z nazwiska: przy takiej konwencji dla dwóch użytkowników `Jan Nowak` można utworzyć konta `Jann` oraz `Janno`.

(d) Jeżeli istotne jest rozróżnianie pracowników tymczasowych, ich konta można odróżniać poprzez dodanie prefiksu w postaci litery `T` i myślnika, np. `T-Janno`.

2. **Ochrona kont użytkownika przy pomocy hasła**

W celu ochrony przed nieautoryzowanym dostępem do komputera lub zasobów domeny, dla każdego konta użytkownika należy zdefiniować hasło. Hasło to musi być skomplikowane, aby

zapobiec sytuacji, w której dostęp do zasobów otrzymają osoby niepożądane. Wskazówki do tworzenia haseł:

(a) Należy zawsze definiować hasło dla konta administratora, aby zapobiec niepowołanemu dostępowi do tego konta.

(b) Należy określić, kto: administrator, czy użytkownicy będą definiować hasła do kont. Administrator może zdefiniować hasła użytkowników i nie pozwolić na ich zmianę, bądź też każdy użytkownik może definiować swoje hasło przy pierwszym logowaniu.

(c) Należy zawsze definiować hasła stosunkowo skomplikowane, utrudniające ich odgadnięcie. Nie wolno zabezpieczać kont hasłami łatwymi do odgadnięcia, takimi, jak nazwisko czy imię ulubionego zwierzaka. Warto do hasła używać kombinacji dużych i małych liter oraz znaków specjalnych. Hasło może mieć do 127 znaków, ale przyjmuje się, że bezpieczne hasło powinno mieć co najmniej 8 znaków.

Silne hasło

Hasła stanowią pierwszą linię obrony przed nieautoryzowanym dostępem do komputera. Im silniejsze hasło, tym lepsze zabezpieczenie komputera przed działalnością hakerów i złośliwego oprogramowania. Należy upewnić się, że dla wszystkich kont na komputerze zostały ustawione silne hasła. Silne hasło ma co najmniej 8 znaków długości. Nie zawiera nazwy użytkownika, imienia, nazwiska ani nazwy firmy. Nie zawiera całego wyrazu. Różni się znacznie od haseł poprzednio używanych przez użytkownika. Zawiera wielkie i małe litery, liczby, znaki specjalne oraz spację. Do budowy silnego hasła można użyć znaków ASCII. Na przykład hasło `Hello2U!` zawiera zalecane znaki, ale jest słabe, ponieważ zawiera całe słowo. Hasło `H3 l#l-0:2,U!` jest silniejsze, ponieważ niektóre litery w całym słowie zostały zastąpione przez liczby a także hasło zawiera spacje i inne znaki.

Ustalanie zasad dotyczących hasła

Podczas tworzenia nowego konta użytkownika, dostępne są następujące opcje dotyczące hasła:

- `Użytkownik musi zmienić hasło przy następnym logowaniu`. Jeżeli pole będzie zaznaczone, tylko użytkownik będzie znał swoje hasło – po jego zmianie przy pierwszym logowaniu. W ten sposób można wymusić na użytkowniku zmianę hasła.
- `Użytkownik nie może zmienić hasła`. Jeżeli pole to jest zaznaczone, administrator komputera zachowuje kontrolę nad hasłem. Pole to należy zaznaczyć w przypadku, gdy administrator chce sam ustalać hasła użytkowników lub też w przypadku, gdy z konta korzysta kilka osób (np. poprzez konto `Gość`).
- `Hasło nigdy nie wygasa`. W przypadku zaznaczenia, nie będzie potrzeby zmiany hasła.
- `Konto jest wyłączone`. Zaznaczając to pole można zablokować konto – na przykład dla pracownika, który jeszcze nie rozpoczął pracy.
- `Konto jest zablokwane`. Oznacza, że użytkownik nie może się zalogować do komputera lokalnego. Jeśli pole wyboru jest niedostępne i wyczyszczone, konto nie jest aktualnie zablokowane. Jeśli pole wyboru jest dostępne i zaznaczone, konto jest aktualnie zablokowane. Aby odblokować konto, można wyczyścić pole wyboru. Tej opcji nie można użyć do zablokowania konta. Istnieje tylko jeden sposób, aby zablokować konto: użytkownik próbuje się zalogować więcej razy niż to określono w ustawieniu zasady `Zasady zabezpieczeń lokalnych` → `Ustawienia zabezbieczeń` → `Zasady konta` → `Zasady blokady konta` → `Próg blokady konta`. Aby uniemożliwić korzystanie z konta, należy je wyłączyć.

UWAGA! Jeżeli zaznaczona jest opcja `Użytkownik musi zmienić hasło przy następnym logowaniu`, nadpisuje ona opcję `Hasło nigdy nie wygasa`.

Warto zapamiętać

(a) W celu zapewnienia wyższego stopnia bezpieczeństwa, należy zmienić nazwę wbudowanego konta administratora. Nazwę należy zdefiniować tak, aby nie kojarzyła się z kontem administratora. Dzięki temu dostęp do tego konta przez nieuprawnionych użytkowników zostanie znacznie utrudniony.

(b) Utworzyć konto dla siebie i zdefiniować dla niego uprawnienia administratorskie. Konta tego należy używać jedynie do wykonywaniu zadań administratorskich.

(c) Utworzyć konto, które będzie wykorzystywane do wykonywania codziennych zadań. Na konto, posiadające uprawnienia administratora należy się logować tylko w przypadku, gdy są do wykonania jakieś zadania administratorskie.

(d) W sieciach o niskim poziomie bezpieczeństwa można odblokować konto `Gość`. Należy jednak koniecznie zdefiniować dla tego konta hasło. Konto to domyślnie jest wyłączone.

(e) Można zawsze wymagać od nowego użytkownika, aby zmieniał hasło przy pierwszym logowaniu. Dzięki temu administrator może być pewien, że hasła są unikalne i znane tylko użytkownikom. Metoda ma tę wadę, że użytkownicy często wybierają hasła trywialne do odgadnięcia, co ułatwia włamanie metodą zgadywania hasła.

(f) Innym rozwiązaniem jest generowanie losowych haseł dla wszystkich użytkowników. Hasła te powinny składać się z kombinacji znaków i cyfr. Tworzenie takich haseł zwiększa poziom bezpieczeństwa w sieci, często jednak użytkownicy, jeżeli mają trudności z zapamiętaniem haseł, zapisują je na przechowywanych obok komputera kartkach. Naraża to oczywiście na niebezpieczeństwo odczytania takiego hasła przez osobę nieuprawnioną.

(g) Należy bezwzględnie zabezpieczać każde konto hasłem, nawet, jeżeli użytkownik będzie musiał zmienić to hasło przy pierwszym logowaniu.

(h) Warto określić datę wygaśnięcia konta w przypadku, gdy będzie ono wykorzystywane tylko przez pewien określony czas (np. konta pracowników tymczasowych).

Zasady haseł

Można ustawić pewne zasady nałożone na hasła.

`Hasło musi spełniać wymagania co do złożoności`

- hasło powinno liczyć co najmniej sześć znaków
- zawierać kombinację przynajmniej trzech poniższych rodzajów znaków: wielkie litery, małe litery, cyfry lub symbole (znaki interpunkcyjne)
- nie może zawierać nazwy użytkownika ani nazwy wyświetlanej

`Wymuszaj tworzenie historii haseł.` Zapobiega utworzeniu przez użytkownika nowego hasła, będącego powtórzeniem bieżącego lub ostatnio używanego hasła. Aby określić, ile haseł jest zapamiętywanych, należy podać wartość. Na przykład wartość równa 1 oznacza, że tylko ostatnie hasło będzie zapamiętywane, natomiast wartość równa 5 oznacza, że zapamiętywanych będzie 5 poprzednich haseł.

`Maksymalny okres ważności hasła.` Ustawia maksymalną liczbę dni, podczas których hasło jest prawidłowe. Po upłynięciu tego okresu użytkownik musi zmienić hasło. Wiek hasła należy ustawić maksymalnie na 70 dni. Ustawienie zbyt dużej liczby dni zwiększa szanse hakerów na złamanie hasła. Ustawienie zbyt małej liczby dni może z kolei być frustrujące dla użytkowników, którzy będą zmuszeni do zbyt częstej zmiany haseł.

`Minimalny okres ważności hasła.` Ustawia minimalną liczbę dni, po upływie których użytkownik może zmienić hasło. Należy ustawić wiek hasła na przynajmniej 1 dzień. Dzięki temu użytkownik może zmieniać hasło tylko raz dziennie. Ułatwia to wymuszenie innych ustawień. Na przykład, jeśli zapamiętywanych jest pięć ostatnich haseł, to ustawienie zapewnia, że upłynie przynajmniej 5 dni, zanim użytkownik będzie mógł ponownie użyć oryginalnego hasła. Jeśli minimalny wiek hasła wynosi 0, użytkownik może zmieniać hasło 6 razy dziennie i ponownie użyć oryginalnego hasła jeszcze tego samego dnia.

`Minimalna długość hasła.` Określa najmniejszą dopuszczalną liczbę znaków w haśle. Hasło powinno liczyć od 8 do 12 znaków (pod warunkiem, że spełnia również wymagania co do złożoności). Dłuższe hasło jest trudniejsze do złamania niż krótsze, przy założeniu, że hasło nie jest słowem ani popularną frazą. Jeśli jednak nie ma obaw co do innych osób w biurze lub w domu, które mogą korzystać z komputera, brak hasła zapewnia lepszą ochronę przez próbą włamania do komputera ze strony hakera przy użyciu Internetu lub innej sieci niż łatwe do odgadnięcia hasło. W przypadku braku hasła system Windows automatycznie udaremni próbę logowania do komputera z Internetu lub innej sieci.

`Przechowuj hasła przy użyciu szyfrowania odwracalnego.` Przechowuje hasło bez szyfrowania. Nie należy korzystać z tego ustawienia, jeśli nie wymaga tego używany program.

3. **Dostosowywanie profilu użytkownika**

W systemie Windows 7 środowisko pracy użytkownika określane jest przez profil użytkownika. Z powodów bezpieczeństwa w systemie Windows 7 wymagane jest, aby dla każdego konta użytkownika mającego dostęp do systemu, był definiowany profil. W profilu użytkownika zawarte są wszystkie ustawienia, które użytkownik może zdefiniować w środowisku systemu Windows 7. W profilu użytkownika przechowywane są ustawienia ekranu, myszy, dźwięku oraz ustawienia regionalne i połączenia sieciowe. Profil użytkownika można tak skonfigurować, aby był on kopiowany na każdy komputer, z którego użytkownik się loguje.

Profil użytkownika jest tworzony przy pierwszym logowaniu się użytkownika. Wszystkie ustawienia użytkownika są automatycznie zachowywane w folderze tworzonym dla każdego użytkownika (domyślnie jest to folder `C:\Użytkownicy\nazwa_użytkownika`. Podczas wylogowywania się użytkownika, jego profil jest uaktualniany. Procedura ta odbywa się na komputerze, z którego użytkownik był zalogowany. W profilu użytkownika przechowywane są ustawienia jego środowiska pracy na lokalnym komputerze. Tylko administrator może zmienić obowiązkowy profil użytkownika. Wyróżniane są następujące profile użytkownika:

(a) Domyślny profil użytkownika. Służy jako podstawowy profil dla wszystkich użytkowników. Każdy profil jest początkowo kopią domyślnego profilu przechowywanego na komputerze pracującym z systemem Windows 7 lub Windows 2008 Server.

(b) Lokalny profil użytkownika. Tworzony jest w chwili pierwszego logowania do komputera i przechowywany jest lokalnie. Wszystkie zmiany dokonane w tym profilu są zapisywane na komputerze, na którym zostały wykonane. Na jednym komputerze może istnieć wiele profili lokalnych. Lokalizacja: `C:\Użytkownicy\nazwa_użytkownika\NETUSER.DAT`.

(c) Mobilny profil użytkownika. Tworzony jest przez administratora i przechowywany na serwerze. Profil ten jest dostępny z dowolnego komputera, do którego loguje się użytkownik. Wszelkie zmiany w profilu zapisywane są na serwerze w chwili wylogowywania.

(d) Obowiązkowy profil użytkownika. Tworzony jest przez administratora. Zdefiniowane są w nim określone ustawienia użytkownika lub użytkowników. Może to być profil lokalny lub wędrujący. Profil obowiązkowy nie pozwala na zapisanie żadnych zmian dokonanych przez użytkowników. Użytkownicy mogą zmieniać ustawienia profilu po zalogowaniu się, ale podczas wylogowywania się żadne zmiany nie zostaną zapisane.

Profil użytkownika można przechowywać na serwerze, aby był on dostępny na dowolnym komputerze w sieci. Profil mobilny oraz obowiązkowy jest przechowywany centralnie na serwerze, aby użytkownik mógł pracować w takim samym środowisku, niezależnie od komputera, do którego jest zalogowany.

UWAGA! Plik `NTUSER.DAT` zawiera klucze rejestru z informacjami o koncie użytkownika oraz ustawienia profilu. Plik ten znajduje się w folderze profilu użytkownika.

UWAGA! Plik `NTUSER.DAT` posiada atrybut `Ukryty (Hidden)` i domyślnie nie jest widoczny w `Eksploratorze Windows`.

Tworzenie folderów macierzystych
Użytkownicy mogą przechowywać swoje dane w pojedynczej, centralnej lokalizacji. Foldery macierzyste nie są częścią profili użytkowników, więc nie mają wpływu na proces logowania użytkowników. Można je umieścić na serwerze sieciowym. Uwagi do określania położenia folderów macierzystych:

(a) Możliwość wykonania kopii zapasowych. Jeśli ochrona przed utratą danych jest bardzo istotnym problemem, warto rozważyć stworzenie folderów macierzystych na serwerze. Zapewnia to łatwość tworzenia kopii zapasowych i daje pewność, że zarchiwizowane zostały wszystkie dane. Jeżeli foldery macierzyste będą przechowywane na komputerach lokalnych, archiwizację należy wykonać na każdym komputerze oddzielnie.

(b) Ilość miejsca na dysku serwera. Serwer musi mieć dostateczną ilość miejsca do przechowywania danych. Istnieje możliwość kontrolowania wykorzystania dysku przez użytkowników.

(c) Dostateczna ilość miejsca na komputerze użytkownika. Jeżeli komputer użytkownika dysponuje niewielkim dyskiem twardym, foldery macierzyste należy założyć na serwerze.

(d) Wydajność sieci. Lokalne przechowywanie folderów macierzystych powoduje odciążenie sieci.

3 Przebieg ćwiczenia

1. Sprawdzić możliwości tworzenia kont użytkowników:
   (a) `Start` → `Panel sterowania` → `Konta użytkowników i Filtr rodzinny` → `Konta użytkowników` → `Zarządzaj innym kontem` → `Utwórz nowe konto`
   (b) `Start` → `Panel sterowania` → `System i zabezpieczenia` → `Narzędzia administracyjne` → `Zarządzanie komputerem` → `Narzędzia systemowe` → `Użytkownicy i grupy lokalne` → `Użytkownicy`
   (c) `Start` → `Komputer` następnie kliknąć prwym przyciskiem myszy i wybrać pozycję `Zarządzaj` a dalej jak w poprzednim podpunkcie.
   (d) Prawym przyciskiem myszy kliknąć na przycisku `Start` a następnie wybieramy `Właściwości`. Na karcie `Menu start` wybieramy przycisk `Dostosuj...`. Szukamy opcję `Systemowe narzędzia administracyjne` i zaznacz opcję `Wyświetl w menu Wszystkie programy i w menu Start`. Następnie w menu `Start` pojawi się pozycja `Narzędzia administracyjne` a w niej opcja `Zarządzanie komputerem`, którą już znamy z wcześniejszych podpunktów.

2. Tworzenie lokalnych kont użytkowników
   (a) Zaloguj się jako administrator.
   (b) Przejrzyj jakie mamy dostępne konta w systemie: `Zarządzanie komputerem` → `Narzędzia systemowe` → `Użytkownicy i grupy lokalne` → `Użytkownicy`.
   (c) Ustaw się myszką na folderze `Użytkownicy` i prawym przyciskiem myszy wybierz *Pomoc*. Zapoznaj się z pomocą dotyczącą zagadnienia: *Użytkownicy i grupy lokalne* → *Pojęcia* → *Opis przystawki Użytkownicy i grupy lokalne* → *Konta użytkowników lokalnych*.
   (d) Przy pomocy aplikacji `Zarządzanie komputerem` utwórz konto `Uzytkownik1`. Konto nie powinno posiadać uprawnień administracyjnych. Dlaczego konto `Gość` jest oznaczone czarną strzałką w dół?
   (e) Zaloguj się jako `Uzytkownik1`. Utwórz nowe konto, korzystając z aplikacji `Zarządzanie komputerem`, o nazwie `Kierownik` z opisem `Kierownik działu`. Dlaczego pojawia się komunikat o błędzie?
   (f) Używając polecenia `Uruchom jako administrator` (kliknąć prawym przyciskiem myszy na program `Zarządzanie komputerem`) utwórz konto `Kierownik`. Jaki użytkownik może założyć nowe konto?
   (g) Zapoznaj się z systemem pomocy w aplikacji `Zarządzanie komputerem`. Menu *Pomoc* → *Tematy Pomocy* → *Użytkownicy i grupy lokalne* i odpowiedz na pytania:

i. Dlaczego nie należy uruchamiać komputera jako administrator?

ii. Dlaczego do zwykłej pracy na codzień nie powinno się korzystać z konta, które ma uprawnienia administratorskie?

(h) Utworz konto o nazwie `Kierownik2` poprzez `Panel sterowania` → `Dodaj lub usuń konta użytkowników`. Jaki pojawia się wówczas komunikat i dlaczego?

(i) Uruchomić `Wiersz polecenia`. W tym celu wykonaj: `Start` → `Wyszukaj programy i pliki` a następnie wpisz polecenie `cmd` i naciśnij klawisz Enter. Po pojawieniu się okna wiersza polecenia wpisać następującą komendę: `net help user` a następnie `net user`.

(j) Aby móc dodawać, usuwać lub modyfikować użytkowników z lini komend należy uruchomić wiersz polecenia jako administrator. Z linii komend można to zrobić poprzez polecenie: `runas /user:administrator cmd`. W celu uzyskania pomocy do polecenia `runas` wpisz następujące polecenie: `runas /?`.

(k) Zaloguj się jako administrator i usuń konta `Uzytkownik1` i `Kierownik` przy pomocy programu `Zarządzanie komputerem`.

3. Utwórzmy kilka kont przynależących do różnych grup przy pomocy programu `Zarządzanie komputerem`:

(a) Przejrzyj jakie mamy dostępne grupy w systemie: `Zarządzanie komputerem` → `Narzędzia systemowe` → `Użytkownicy i grupy lokalne` → `Grupy`.

(b) Ustaw się myszką na folderze `Grupy` i prawym przyciskiem myszy wybierz *Pomoc*. Zapoznaj się z pomocą dotyczącą zagadnienia: *Użytkownicy i grupy lokalne* → *Pojęcia* → *Opis przystawki Użytkownicy i grupy lokalne* → *Domyślne grupy lokalne*.

(c) Utwórz konta: `Student1` (Użytkownicy zaawansowansowani), `Student2` (Użytkownicy), `Student3` (Goście) oraz `Student4` (Administratorzy).

(d) Logując się na poszczególne konta sprawdź jakie czynności mogą wykonywać poszczególni użytkownicy. Czy wszyscy użytkownicy mają dostęp do plików systemowych, aplikacji panelu sterowania i innych zasobów? Czy `Student3` po wejściu do katalogu `C:\Windows` może coś w nim dodadać (utworzyć pliki, katalogi) lub usunąć z niego? Dlaczego?

(e) Zaloguj się jako administrator i usuń konta założone w ppkt. 3c przy pomocy programu `Zarządzanie komputerem`.

(f) Uruchomić `Wiersz polecenia` i wpisać następującą komendę: `net help localgroup` a następnie `net localgroup`.

4. Zasady tworzenia haseł

(a) Zasady dotyczace hasła można ustawić za pomocą aplikacji dostępnej w następującej lokalizacji:

- `Start` → `Narzędzia administracyjne` → `Zasady zabezpieczeń lokalnych` → `Ustawienia zabezpieczeń` → `Zasady konta` → `Zasady haseł`.
- `Start` → `Panel sterowania` → `System i zabezpieczenia` → `Narzędzia administracyjne` → `Zasady zabezpieczeń lokalnych` → `Ustawienia zabezpieczeń` → `Zasady konta` → `Zasady haseł`.
- Uruchomić `Wiersz polecenia` i wpisać następującą komendę: `net help accounts` a następnie `net accounts`.

(b) Dla każdej z opcji wybrać prawym przyciskiem myszy `Właściwości`. W pierwszej karcie mamy pokazane odpowiednie atrybuty w zależności od rodzaju, będzie to informacja o wartości lub stanie tej właściwości. Na drugiej karcie zatytułowanej `Wyjaśnienie` mamy opis tej właściwości. Proszę zapoznać sie z opisem dla każdej z tych opcji.

(c) Włączyć opcje dotyczące komplikacji hasła, długość min 8 znaków oraz ważność hasła ustawić na 14 dni. Sprawdzić czy można podać hasło nie spełniające powższych wymagań.

(d) Czym różnią się zasady lokalne od efektywnych?

5. Zasady blokady konta

(a) Zasady dotyczące blokady konta można ustawić za pomocą aplikacji dostępnej w następującej lokalizacji:

- `Start` → `Narzędzia administracyjne` → `Zasady zabezpieczeń lokalnych` → `Ustawienia zabezpieczeń` → `Zasady konta` → `Zasady blokady konta`.
- `Start` → `Panel sterowania` → `System i zabezpieczenia` → `Narzędzia administracyjne` → `Zasady zabezpieczeń lokalnych` → `Ustawienia zabezpieczeń` → `Zasady konta` → `Zasady blokady konta`.

(b) Dla każdej z opcji wybrać prawym przyciskiem myszy `Właściwości`. W pierwszej karcie mamy pokazane odpowiednie atrybuty w zależności od rodzaju, będzie to informacja o wartości lub stanie tej właściwości. Na drugiej karcie zatytułowanej `Wyjaśnienie` mamy opis tej właściwości. Proszę zapoznać sie z opisem dla każdej z tych opcji.

(c) Włączyć opcje blokady konta tak, aby było blokowane na 5 minut po wprowadzeniu 3 błędnych haseł. Sprawdzić działanie włączonych mechanizmów

6. Sprawdzanie profilu użytkownika i tworzenie folderów macierzystych

(a) Zaloguj się jako administrator i utwórz konto `zaoczny` (użytkownik standardowy).

(b) Po dwukrotnym kliknięciu w użytkownika `zaoczny` pojawi się okno właściwości dla tego konta. Proszę kliknąć przycisk `Pomoc`, który jest na dole tego ekranu i zapoznać się z informacjami tam zawartymi w szczególności: `Użytkownicy i grupy lokalne` → `Interfejs użytkownika: Użytkownicy i grupy lokalne` → `Arkusz właściwości <Użytkownik> - Profil`

(c) Przetestuj wszystkie możliwe scenariusze ustalania przez administratora zasad dotyczących hasła: `Użytkownik musi zmienić hasło przy następnym logowaniu`, `Użytkownik nie może zmienić hasła`, `Hasło nigdy nie wygasa`.

(d) Sprawdź, czy w systemie powstał profil użytkownika `zaoczny`. Sprawdzić zawartość folderu `C:\Użytkownicy\zaoczny`.

(e) Sprwdź profile i możliwość ich modyfikacji w:

i. Wybierz `Właściwości` z `Komputer`, następnie `Zaawansowane ustawienia systemu` i dalej na środku karty `Zaawansowane` wybrać `Profile użytkownika` → `Ustawienia`.

ii. `Panel sterowania` → `Konta użytkowników i Filtr rodzinny` → `Konta użytkowników` → `Skonfiguruj zaawansowane właściwości profilu użytkownika`

(f) Ustaw się myszką na koncie `zaoczny` w `Zarządzaniu komputerem` i prawym przyciskiem myszy wybierz *Pomoc*. Zapoznaj się z pomocą dotyczącą zagadnienia: *Użytkownicy i grupy lokalne* → *Pojęcia* → *Administrowanie użytkownikami i grupami lokalnymi* → *Zarządzanie plikami dla kont użytkowników lokalnych.*

(g) Utwórz folder `C:\Student zaoczny` i przypisz go jako folder macierzysty użytkownikowi `zaoczny`. Kto może modyfikować zawartosć tego folderu?

(h) Przejdź do folderu `C:\Użytkownicy\zaoczny` i skopjuj go jako administrator na pulpit pod nazwą `zaoczny_kopia`.

(i) Zaloguj się jako administrator i usuń konto `zaoczny` poprzez `Panel sterowania` → `Dodaj lub usuń konta użytkowników` → `zaoczny` → `Usuń konto` a następnie zapoznaj się z oknem które się pojawi.

(j) Po wybraniu opcji `Usuń konto` a następnie `Zachowaj pliki` z poprzedniego podpunktu, porównaj wielkość i zawartość folderów `zaoczny_kopia` i `zaoczny` po wykonaniu tej operacji.

(k) Sprawdź, czy profil tego użytkownika został usunięty z systemu tak jak to było zrobione w podpunktach 6d i 6e.

4 Przykładowe pytania

1. Co to jest konto użytkownika?
2. Dlaczego nie powinno pracować się na koncie z uprawnieniami administratora?
3. Wymień nazwy kont wbudowanych i odopwiedz na pytanie czy można zmienić im nazwy lub czy można je usunąć?
4. Co to jest profil użytkownika i jakie mamy rodzaje tychże profili?

5. Co to jest baza SAM? Co w niej jest przechowywane i gdzie ona się znajduje (podaj ścieżkę)?
6. Po co są foldery macierzyste i czy folder macierzysty, to to samo co profil użytkownika?
7. W jakim pliku przechowywane są ustawienia o profilu użytkownika oraz co jeszcze jest w nim przechowywane? Gdzie ten plik jest przechowywany (podaj ścieżkę)?

Literatura

[1] Jim Boyce. *Windows 7 PL. Biblia.* Helion, 2010.

[2] Preppernau Joan i Cox Joyce. *Windows 7 krok po kroku.* Wydawnictwo RM, 2010.

[3] Danuta Mendrala i Marcin Szeliga. *Windows 7 PL.* Helion, 2009.

[4] Paul McFedries. *Windows 7 PL. Księga eksperta.* Helion, 2009.

[5] Andrzej Szeląg. *Windows 7 PL. Zaawansowana administracja systemem.* Helion, 2009.

[6] Witold Wrotek. *Rejestr Windows 7. Praktyczne przykłady.* Helion, 2010.